IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UBIQUITI NETWORKS, INC., *Plaintiff,* v. CAMBIUM NETWORKS, INC.; CAMBIUM NETWORKS, LTD.; BLIP NETWORKS, LLC; WINNCOM TECHNOLOGIES, INC.; SAKID AHMED; and DMITRY MOISEEV. *Defendants*.	Civil Action No.: 1:18-cv-05369 **JURY TRIAL DEMANDED**

COMPLAINT

Plaintiff Ubiquiti Networks, Inc. ("Plaintiff" or "Ubiquiti") brings this action against Defendants Cambium Networks, Inc. ("Cambium"), Cambium Networks, Ltd. ("Cambium Networks"), Blip Networks, LLC ("Blip"), Winncom Technologies, Inc. ("Winncom"), Sakid Ahmed, and Dmitry Moiseev and hereby alleges as follows:

NATURE OF THE ACTION

1. This is a Complaint for injunctive relief and damages based on Cambium's intentional, commercially motivated, unauthorized access, reverse engineering and hacking of Ubiquiti's M-series wireless devices and trafficking in hacked firmware that deletes, modifies, and makes unauthorized copies of portions of the Ubiquiti firmware on the Ubiquiti M-series devices, eliminates Ubiquiti copyright notices to conceal Cambium's infringement, eliminates firmware restrictions Ubiquiti put in place to ensure operation in conformity with Federal Communications Commission ("FCC") requirements and licenses, and circumvents access control measures on the

Ubiquiti M-series devices, all in violation of the Computer Fraud and Abuse Act ("CFAA"), the Digital Millennium Copyright Act ("DMCA"), the Illinois Computer Crime Prevention Law, the Copyright Act, various state laws and the Ubiquiti firmware license agreements. Cambium's promotion and distribution of the hacked firmware as a product called Elevate (the "Hacked Firmware") is based on flagrant misrepresentations and false advertising in violation of the Lanham Act and state competition laws, and tortiously interferes with Ubiquiti's license agreements with Ubiquiti customers and Ubiquiti's prospective customers and business relationships. Once hacked with the Hacked Firmware, Ubiquiti M-series devices thereafter violate FCC rules and regulations and FCC licenses for the equipment.

2. The sale and marketing of the Hacked Firmware was carried out through an elaborate scheme of mail and wire fraud involving material misrepresentations and omissions regarding the nature of the Hacked Firmware, willful copyright infringement, and misappropriation of Ubiquiti's time, money, brand recognition, and good will established with existing and prospective customers. Cambium, Cambium Networks, Sakid Ahmed—Vice President of Engineering at Cambium Networks, Dmitry Moiseev—Project Engineer at Cambium Networks, and Winncom (collectively, the "Hacking Enterprise") conspired together and with co-conspirator Blip to defraud Ubiquiti customers and ensure financial gain in connection with marketing, sale, distribution, and use of the Hacked Firmware.

PARTIES

3. Plaintiff Ubiquiti is a corporation organized under the laws of the State of Delaware, with its principal place of business at 685 Third Avenue, 27th Floor, New York, New York 10017.

4. Defendant Cambium is a corporation organized under the laws of the State of Delaware, with its principal place of business at 3800 Golf Road, Suite 360, Rolling Meadows, Illinois 60008.

5. Defendant Cambium Networks is a British limited liability company with its principal place of business in England. Cambium Networks is the parent company of Cambium.

6. Defendant Blip is an Illinois limited liability company, with its principal place of business at 6 Sharp Rock Road, Ava, Illinois 62907-2528.

7. Defendant Winncom is an Ohio corporation, with its principal place of business at 28900 Fountain Parkway # B, Solon, Ohio 44139-4383.

8. Defendant Sakid Ahmed is the Vice President of Engineering at Cambium Networks and a resident of Chicago, Illinois.

9. Defendant Dmitry Moiseev is a Project Engineer at Cambium Networks and a resident of Hoffman Estates, Illinois.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over Ubiquiti's claims arising under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, *et seq.*, the claims arising under the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1961 *et seq.* ("RICO"), the Lanham Act, 15 U.S.C. § 1125 *et seq.*, and the Copyright Act, 17 U.S.C. § 101 *et seq.* pursuant to this Court's federal question jurisdiction under 28 U.S.C. § 1331. This Court also has supplemental jurisdiction over all other claims asserted herein pursuant to 28 U.S.C. § 1367 because those claims are so related to the claims brought under the federal statutes so as to form part of the same case or controversy.

11. This Court has personal jurisdiction over Defendant Cambium. Cambium is registered to do business in the State of Illinois and has a regular and established place of business

in Illinois and this District at 3800 Golf Road, Suite 360, Rolling Meadows, Illinois 60008, and is and has been doing business in Illinois and this District at all times relevant hereto.

12. This Court has personal jurisdiction over Defendants Sakid Ahmed and Dmitry Moiseev, Illinois residents who live, work, are employed, and carried out acts described herein within the Northern District of Illinois.

13. This Court has personal jurisdiction over Defendants because directly or through intermediaries, they have committed acts within or directed at Illinois, causing harm herein and giving rise to this action, and/or have established minimum contacts with Illinois such that the exercise of jurisdiction would not offend traditional notions of fair play and substantial justice.

14. Venue is proper in this Court because Defendants Cambium, Ahmed, Moiseev, and Blip reside or may be found in this District. *See* 28 U.S.C. §§ 1391(b) & (c).

15. Venue is also proper because a substantial part of the events and omissions giving rise to the instant action occurred within this District. Unlawful and improper conduct including the violations of the CFAA, copyright infringement, and fraudulent mailing and interstate wire communications have occurred and originated within this District.

16. Venue is also proper pursuant to 18 U.S.C. § 1965 and 28 U.S.C. § 1391 because Defendants are subject to personal jurisdiction in this District.

FACTUAL ALLEGATIONS

Ubiquiti and Its Products

17. Founded in June 2005, Ubiquiti is a next generation communications technology company that designs and develops, among other things, proprietary wireless networking technologies. Ubiquiti's products and solutions have bridged the digital divide between rural and urban markets by fundamentally changing the economics of deploying high performance networking solutions in underserved and underpenetrated markets globally. Ubiquiti's technology

platforms focus on delivering industry-leading performance, compelling price-performing characteristics and an unparalleled user experience. Ubiquiti has reduced high product and network deployment costs and other business model inefficiencies to enable rapid market adoption of its products and solutions in rural and emerging markets.

18. Ubiquiti has expended considerable time and resources to advertise and promote its products and brand throughout the world. In addition to traditional advertising, Ubiquiti hosts a Ubiquiti Network Community Forum for users of Ubiquiti products who spread information about the products by word of mouth.

19. Over the last eight years, Ubiquiti has spent over 500 million dollars investing in its proprietary products, developing its distribution network, and creating goodwill in the marketplace.

20. Ubiquiti has received substantial unsolicited accolades and press for its successful broadband product line. In 2007, Ubiquiti received significant attention when a group of Italian amateur radio operators set a distance world record for point-to-point links in the 5.8 GHz spectrum using Ubiquiti cards and antennas. Ubiquiti received the Wireless Internet Service Providers Association ("WISPA") Manufacturer of the Year awards in 2010, 2011, 2014, and 2016.

Ubiquiti M-Series Devices

21. Ubiquiti's extensive broadband product line includes Ubiquiti's M-series devices: the NanoStation M, NanoStation Loco M (collectively, "NanoStations"), which are wireless "customer premises equipment" that permit outdoor throughput; the NanoBridge M-series, the NanoBeam M-series and the PowerBeam M-series, which are all wireless bridges that wirelessly rebroadcast packets received; and the AirGrid M-series and the Rocket M-series. The AirGrid M is a broadband wireless device that combines antenna and radio using Ubiquiti's proprietary

Innerfeed technology. The Rocket M is a radio device with enhanced receivers that delivers broadband connectivity through interchangeable antennas.

22. Ubiquiti launched AirMAX® and its M-series product line in 2009. AirMAX incorporates proprietary radio frequency (RF) technology, antenna design, and firmware, which simplify adoption and use of base stations, back haul equipment, and customer premises equipment (CPE).

Ubiquiti M-Series Device Firmware

23. All Ubiquiti AirMAX® products run on Ubiquiti's proprietary airOS® operating system embodied in Ubiquiti's firmware, and under Ubiquiti's proprietary AirMAX® protocol. The AirMAX® logo is present on the packaging of all Ubiquiti AirMAX® products. The airOS® logo appears on screen when a user logs in to the web interface for Ubiquiti M-series devices using the Ubiquiti username and password.

24. The user interface for a M-series device provides a path for upgrading the device firmware. The Ubiquiti user interface is accessed at a designated IP address using a web browser. On the first access to the user interface, the Ubiquiti customer is presented with the "Terms of Use" and the "Ubiquiti Firmware User License Agreement."

25. The unsigned versions of the Ubiquiti firmware include checks for determining whether a firmware upgrade is compatible. Firmware that does not pass the checks is rejected and not installed.

26. Ubiquiti introduced a "signed" version of the airOS® firmware for M-series devices in 2017, including airOS firmware versions 5.6.15 and 6.0.3. The signed versions also allow upgrading, but a more robust signature verification performed by the boot loader verifies new firmware. Users may upgrade with a newer version of Ubiquiti firmware by downloading and installing the newer version.

Ubiquiti Product Packaging, Labeling, and Branding

27. All Ubiquiti AirMAX® product packaging for M-series devices is labeled with Ubiquiti's name and corporate address, Ubiquiti's domain name (www.ubnt.com), the UBIQUITI® trademark and Ubiquiti logo, and the AirMAX® trademark. Each Ubiquiti M-series product is also branded with a trademark associated with that M-series device.

28. Ubiquiti owns registered trademarks used in branding the Ubiquiti M-series products, including: UBIQUITI® - Reg. No. 4,524,111; NANOSTATION® - Reg. No. 4,323,172; NANOBRIDGE® - Reg. No. 4,319,934; NANOBEAM® - Reg. No. 4,519,296; ROCKET® - Reg. No. 4558,159.

29. Ubiquiti owns common law trademarks in other marks used to brand Ubiquiti M-series devices.

30. Ubiquiti owns U.S. Copyright No. TXu001795146 for Ubiquiti firmware airOS version 5.2.1 and U.S. Copyright No. TXu001795146 for Ubiquiti firmware airOS version 5.3. *See* Exhibit A.

31. Ubiquiti also marks products with a unique identifying code called a Media Access Control ID ("MAC ID"). The product packaging and the product labels also contain a unique FCC Identification number approved by the FCC, SWX-M2, which can be used to find information about the manufacturer and the product, including approved frequency ranges, via the FCC website. The packaging and the labels also have the European Union "CE" mark, certifying compliance with European Union safety, health, and environmental protection requirements.

32. In general, Ubiquiti designs and develops each of its products in-house, and uses contract manufacturers to manufacture the products according to Ubiquiti's proprietary designs. Ubiquiti has stringent standards that contract manufacturers are required to meet, and closely

monitors the quality of products that they produce to assure that they meet Ubiquiti's high quality standards.

33. Consumers have come to associate the Ubiquiti brand with its high quality standards and cutting-edge technologies. This is the result of Ubiquiti's extensive investment of time, money, and resources into establishing consumer goodwill and brand recognition.

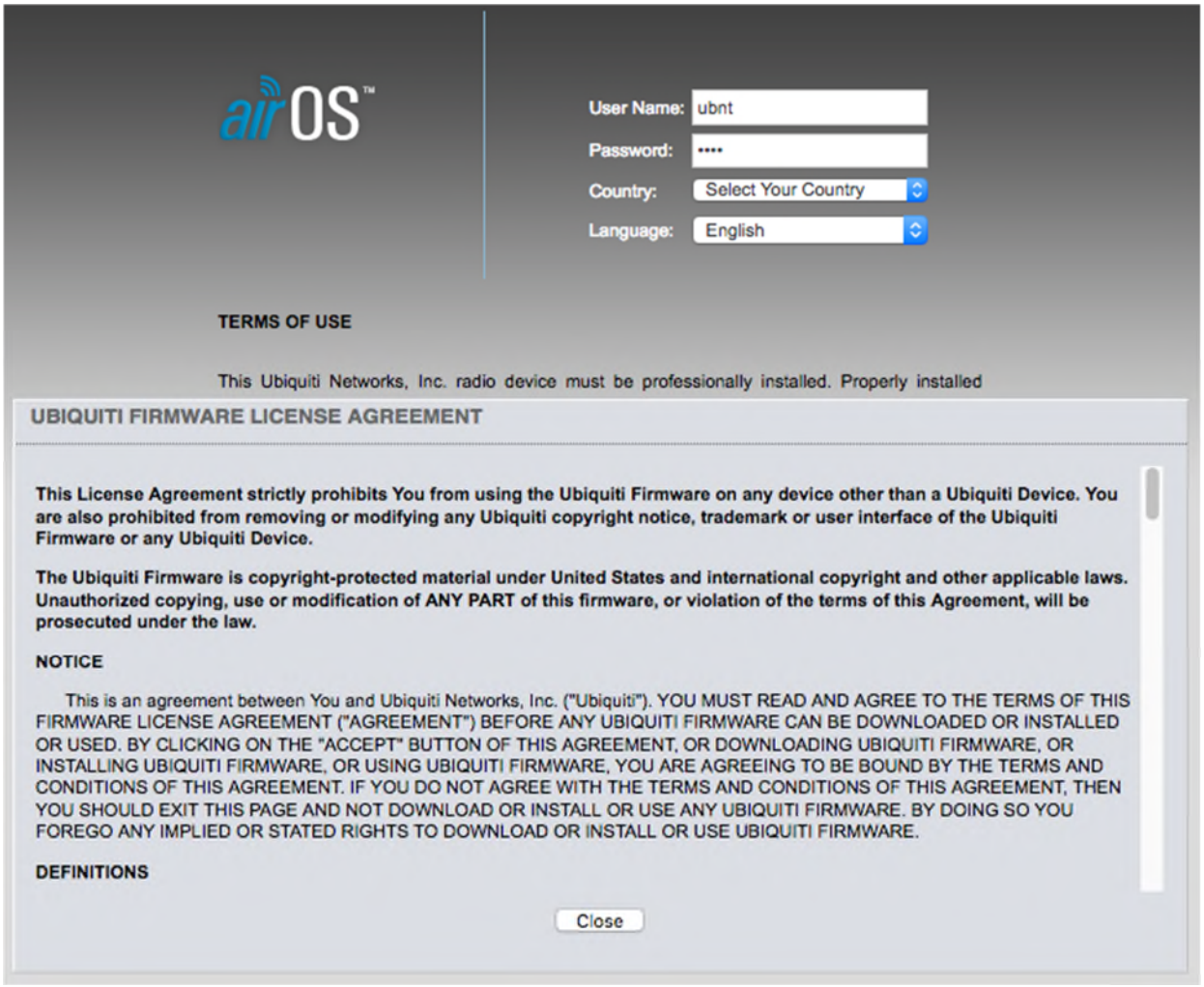
34. Ubiquiti uses a worldwide network of distributors to market and distribute its products. Ubiquiti's products are currently offered in the United States and in over 65 other countries.

35. Ubiquiti primarily sells its M-series devices to wireless Internet service providers (WISPs). WISPs purchase and deploy Ubiquiti M-series products and Ubiquiti access points with which the Ubiquiti M-series products communicate over medium to long range distances to build out wireless broadband networks that span wide geographic areas.

36. The Ubiquiti M-series devices are designed to be affixed by a WISP to structures, such as a building, to establish fixed wireless networks. The Ubiquiti AirMAX® radio protocol is used for wireless communications between Ubiquiti devices.

The Ubiquiti Firmware License Agreements For Its M-Series Products

37. Ubiquiti M-series devices include a user interface for Ubiquiti customers to configure Ubiquiti M-series devices. The user interface is accessed at a designated IP address using a web browser. On the first access, the Ubiquiti customer is presented with the "Terms of Use" and the "Ubiquiti Firmware User License Agreement" as shown below:



The Ubiquiti customer is required to agree to both the Terms of Use and the Ubiquiti Firmware License Agreement, via a checkbox. *See* Terms of Use and the Ubiquiti Firmware License Agreement (Exhibit B).

38. The Ubiquiti Firmware License Agreement requires users to agree to its terms prior to using Ubiquiti firmware and provides in pertinent part:

> This License Agreement strictly prohibits You from using the Ubiquiti Firmware on any device other than a Ubiquiti Device. You are also prohibited from removing or modifying any Ubiquiti copyright notice, trademark or user interface of the Ubiquiti Firmware or any Ubiquiti Device.
>
> The Ubiquiti Firmware is copyright-protected material under United States and international copyright and other applicable

> laws. Unauthorized copying, use or modification of ANY PART of this firmware, or violation of the terms of this Agreement, will be prosecuted under the law.
>
> NOTICE
> This is an agreement between You and Ubiquiti Networks, Inc. ("Ubiquiti"). YOU MUST READ AND AGREE TO THE TERMS OF THIS FIRMWARE LICENSE AGREEMENT ("AGREEMENT") BEFORE ANY UBIQUITI FIRMWARE CAN BE DOWNLOADED OR INSTALLED OR USED. BY CLICKING ON THE "ACCEPT" BUTTON OF THIS AGREEMENT, OR DOWNLOADING UBIQUITI FIRMWARE, OR INSTALLING UBIQUITI FIRMWARE, OR USING UBIQUITI FIRMWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE WITH THE TERMS AND CONDITIONS OF THIS AGREEMENT, THEN YOU SHOULD EXIT THIS PAGE AND NOT DOWNLOAD OR INSTALL OR USE ANY UBIQUITI FIRMWARE. BY DOING SO YOU FOREGO ANY IMPLIED OR STATED RIGHTS TO DOWNLOAD OR INSTALL OR USE UBIQUITI FIRMWARE.

39. The Ubiquiti Firmware License Agreement prohibits, among other things: copying, modifying or reverse engineering the firmware; removing or modifying copyright notices or user interfaces on Ubiquiti devices; and circumventing any software protection mechanisms, including any mechanism used to restrict or control the functionality of the Ubiquiti firmware. The Ubiquiti Firmware License Agreement provides in pertinent part:

> a. **You may not, and shall not permit others to: . . .**
>
> e. copy the Ubiquiti Firmware (except as expressly permitted above), or copy the accompanying documentation;
>
> f. modify, translate, reverse engineer, decompile, disassemble or otherwise attempt (i) to defeat, avoid, bypass, remove, deactivate, or otherwise circumvent any software protection mechanisms in the Ubiquiti Firmware, including without limitation any such mechanism used to restrict or control the functionality of the Ubiquiti Firmware, or (ii) to derive the source code or the underlying ideas, algorithms, structure or organization from the Ubiquiti Firmware (except that the foregoing limitation does not apply to the extent that such activities may not be prohibited under applicable law); or

> g. distribute, rent, transfer or grant any rights in the Ubiquiti Firmware or modifications thereof or accompanying documentation in any form to any person without the prior written consent of Ubiquiti;
>
> h. remove any Ubiquiti copyright notice or Ubiquiti branding from the Ubiquiti Firmware or modify any user interface of the Ubiquiti Firmware or Ubiquiti Device.

40. The Ubiquiti Firmware License Agreement provides for automatic termination in the event that the user violates the Firmware License Agreement, stating in pertinent part:

> Unauthorized copying of the Ubiquiti Firmware or failure to comply with the above restrictions will result in automatic termination of this Agreement and will make available to Ubiquiti other legal remedies. . . . Upon termination of this license for any reason You will destroy all copies of the Ubiquiti Firmware. Any use of the Ubiquiti Firmware after termination is unlawful.

41. Ubiquiti allows its customers to download Ubiquiti firmware updates for use on Ubiquiti M-series devices from the Ubiquiti website, by first agreeing to the terms of an End User License Agreement (EULA). *See* EULA (Exhibit C).

42. The EULA applicable to any Ubiquiti firmware downloaded from the Ubiquiti website, like the Firmware License Agreement, also prohibits removing or modifying copyright notices or user interfaces on Ubiquiti devices, and prohibits unauthorized copying, modification or removal of any part of the Ubiquiti firmware. The EULA also prohibits reverse engineering and circumventing any software protection mechanisms, including any mechanism used to restrict or control the functionality of the Ubiquiti firmware. Violations of the EULA result in automatic termination of the EULA. Ubiquiti's Terms of Use, Firmware License Agreement, and EULA applicable to Ubiquiti firmware are collectively referred to as Ubiquiti's "Firmware License Agreements."

Cambium's Creation of Hacked Firmware Targeting Ubiquiti M-Series Devices, Hacking, Unlawful Conduct, and Fraud

43. On information and belief, prior to November 30, 2016, Cambium acquired one or more Ubiquiti M-series wireless devices and at least one version of Ubiquiti's Air/OS firmware for the unauthorized purposes of reverse engineering the Ubiquiti firmware for M-series devices, accessing proprietary Ubiquiti information embedded in the firmware, copying portions of the firmware, modifying the firmware and user interfaces and developing and trafficking in Hacked Firmware targeting Ubiquiti M-series devices, and capitalizing on Ubiquiti's product development investment and customer goodwill. The Hacked Firmware does all of the following without authorization and in violation of Ubiquiti firmware license agreements:

44. The Hacked Firmware deletes portions of the Ubiquiti firmware and Ubiquiti user interfaces from Ubiquiti M-series devices.

45. The Hacked Firmware selectively modifies and copies portions of Ubiquiti firmware.

46. The Hacked Firmware makes unauthorized access to portions of the firmware that remain on Ubiquiti M-series devices after the hack.

47. The Hacked Firmware replaces the original radio software on Ubiquiti M-series devices with different, unauthorized radio software that causes the devices to stop operating in conformity with FCC requirements and equipment authorizations.

48. The Hacked Firmware circumvents access control measures on M-series devices.

49. On information and belief, Cambium reverse engineered the Ubiquiti firmware stored on M-series devices, in order to study the structure and proprietary aspects of the Ubiquiti firmware to create Hacked Firmware capable of circumventing Ubiquiti's access control mechanisms, including mechanisms used to verify firmware as permissible on M-series devices.

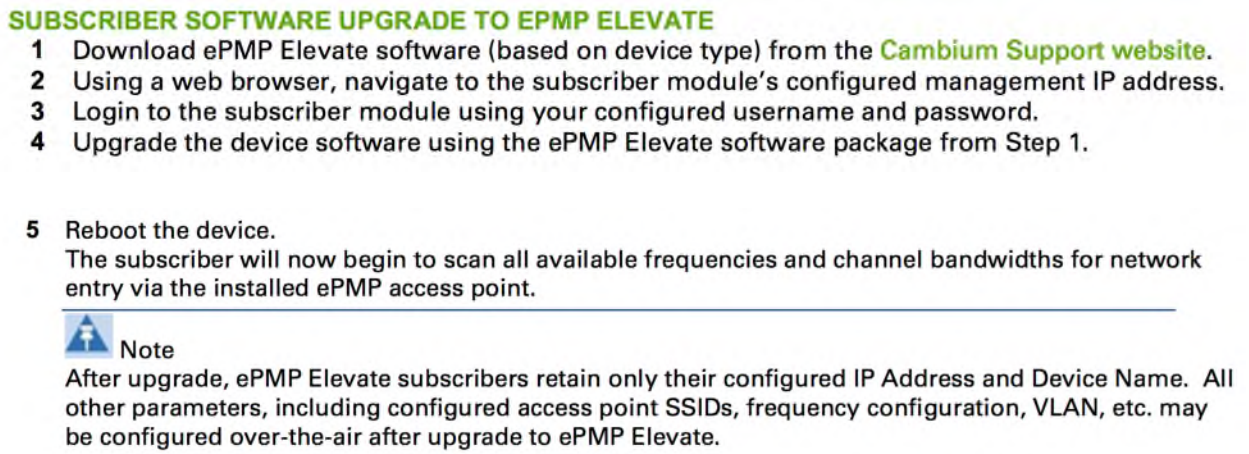
50. The Hacked Firmware removes proprietary Ubiquiti notices on Ubiquiti M-series devices.

51. The Hacked Firmware changes the user interfaces for M-series devices and makes unauthorized use of Ubiquiti trademarks in the user interfaces.

52. The Hacked Firmware renders the Ubiquiti M-series devices incapable of communicating with other Ubiquiti access points using Ubiquiti's radio software and instead causes the hacked Ubiquiti M-series devices only to communicate with Cambium access points.

53. Cambium instructs Ubiquiti licensees and customers to download the Hacked Firmware, open the Ubiquiti user interface on Ubiquiti M-series devices used for configuration, and to install the Hacked Firmware on M-series devices in violation of Ubiquiti firmware license agreements.

54. Cambium directs Ubiquiti's licensees using Ubiquiti M-series products to install the Hacked Firmware on Ubiquiti M-series products by following the ePMP Elevate Quick Start Guide (Exhibit D), excerpted below, as well as by following an online video:



SUBSCRIBER SOFTWARE UPGRADE TO EPMP ELEVATE

1 Download ePMP Elevate software (based on device type) from the Cambium Support website.
2 Using a web browser, navigate to the subscriber module's configured management IP address.
3 Login to the subscriber module using your configured username and password.
4 Upgrade the device software using the ePMP Elevate software package from Step 1.

5 Reboot the device.
The subscriber will now begin to scan all available frequencies and channel bandwidths for network entry via the installed ePMP access point.

Note
After upgrade, ePMP Elevate subscribers retain only their configured IP Address and Device Name. All other parameters, including configured access point SSIDs, frequency configuration, VLAN, etc. may be configured over-the-air after upgrade to ePMP Elevate.

Figure 1 – Elevate firmware update instructions from ePMP Elevate Quick Start Guide v3.2 (p. 5) (Ex. D)

55. Cambium formats the Hacked Firmware to be accepted by Ubiquiti's firmware update process and to hack M-series devices and the installed firmware in violation of Ubiquiti's Firmware License Agreements. Incorrectly formatted firmware is rejected by the Ubiquiti firmware.

56. After a Ubiquiti M-series device is hacked with the Hacked Firmware, the device's entire Ubiquiti user interface is replaced with a Cambium User Interface. This violates the Ubiquiti Firmware License Agreement.

57. Most Ubiquiti trademarks and logos are removed in the hacked User Interface However, Cambium still uses the M-series device trademarks, such as NANOSTATION®, within the hacked User Interface when a NanoStation M5 device has been taken over by the Hacked Firmware.

58. Each page of the Ubiquiti User Interface contains a Ubiquiti copyright notice. Cambium's replacement User Interface removes these notices and instead contains only Cambium Networks copyright notices. The removal of the Ubiquiti copyright notice is a violation of the Ubiquiti Firmware License Agreements.

59. Cambium's installation of the Hacked Firmware on Ubiquiti M-series devices, and such installation on M-series devices by others at Cambium's urging, is a violation of FCC rules.

60. Installation of the Hacked Firmware on Ubiquiti M-series devices modifies the Ubiquiti firmware and causes the Ubiquiti M-series devices to transmit with characteristics that are not allowed by the FCC equipment authorization and FCC rules, or the original Ubiquiti firmware, in violation of the Ubiquiti Firmware License Agreement.

61. Cambium admits that its firmware exceeds the original transmission thresholds:

Known problems or limitations (System Release 3.4)

Tracking Description / Workaround

. . .

14458 [ePMP Elevate 2.4, XM] Cambium Elevate operating Tx Power exceeds original nonCambium software-configured Tx Power by 1.5 – 3 dBm"

See Cambium Release Notes v. 3.5.1 (Exhibit E)

Cambium's Unlawful Promotion and Distribution of Hacked Firmware

62. In selling the Hacked Firmware, Cambium misleads and induces customers to make two significant modifications to two separate Ubiquiti products: (1) the Ubiquiti Firmware and (2) the Ubiquiti M-Series devices. *See generally* Exhibit F (Transcription of Portions of November 30, 2016 ePMP Elevate Webinar).

63. Cambium describes the Hacked Firmware, which it refers to as ePMP Elevate, as "an innovative software solution" that allows customers to "increase performance ***without replacing installed hardware***." (Exhibit G) (emphasis added), https://www.cambiumnetworks.com/products/access/epmp-elevate/.

64. According to Cambium, the ePMP Elevate software is intended to allow fixed wireless broadband networks to gain capabilities of the Cambium Networks' ePMP platform including frequency reuse enabled by GPS Synchronization and Smart Beamforming.

65. As a commercial benefit and cost savings, Cambium promotes the Hacked Firmware as a means to use the existing infrastructure licensed by other companies. The ePMP™ Elevate software product is designed to be used "even on non-Cambium Networks 802.11n-based hardware." (Exhibit H). According to Cambium, "Saving the cost and time of a total network replacement, an operator simply installs an ePMP Access Point and loads ePMP Elevate software onto their deployed subscriber modules." (Ex. G).

66. As material omissions, Cambium fails to tell customers that the use of the Hacked Firmware makes modifications to M-series devices and Ubiquiti firmware that violates Ubiquiti

firmware license agreements, violates FCC requirements and rules, and violates Ubiquiti's intellectual property rights.

67. The Ubiquiti Firmware is modified—portions remain, portions are modified, portions are removed and portions are copied—when the Cambium Hacked Firmware is installed.

68. Cambium officials highlight that the Hacked Firmware modifies the Ubiquiti M-series devices and firmware, and they promote the modification as a commercial benefit. For example, in the ePMP Portfolio Overview (Exhibit I), Cambium's promotional literature notes that the ePMP Elevate software product can "leverage an existing 802.11-based installed network and add synchronization without the cost of replacing the entire network." (Ex. I, Page 7). The Ubiquiti® XW/XM (including the trademark) is also listed as a supported product. (*Id.*).

69. Exhibit J shows a comparison between the user interface for the Ubiquiti PowerBeam M series product taken from the AirOS user guide and the user interface for an "Elevated" Ubiquiti product. The Ubiquiti user interface has a copyright notice on the bottom and features "Genuine Product" along with trademarks for the product name, AirOS and a design. The Cambium user interface eliminates the Ubiquiti copyright notice and replaces it with a Cambium copyright notice. It also makes unauthorized use of the Ubiquiti product name, in this instance the NanoBeam M5.

70. On or about November 30, 2016, Cambium began publicly promoting the Hacked Firmware under the name "Elevate" and "ePMP Elevate" for large scale distribution through a webinar, its website, and other avenues.

71. Cambium has continued to heavily promote the Hacked Firmware in the United States and throughout the world with additional webinars directed at WISPs, and marketing and distribution of literature and web pages through third party distributors, including distributors used

by both Cambium and Ubiquiti. Cambium has marketed the Hacked Firmware at industry conferences attended by WISPs, Cambium, and Ubiquiti and through live educational seminars directed at distributors and WISPs and demonstrating hacking Ubiquiti M-series devices using the Hacked Firmware.

Summary of Cambium's Illicit Conduct

72. Cambium's development, promotion and distribution of the Hacked Firmware violates the Ubiquiti Firmware License Agreements. Through Cambium's widespread promotion and distribution of the Hacked Firmware, Cambium willfully, and with full knowledge of Ubiquiti's proprietary rights, induces third parties, including Ubiquiti customers, to violate the Ubiquiti Firmware License Agreements and to violate Ubiquiti's copyrights and misappropriate Ubiquiti's proprietary information embedded in the firmware by installing and using Hacked Firmware on Ubiquiti M-series devices.

73. The Hacked Firmware, when installed by Cambium, a Cambium distributor or a Ubiquiti customer on a Ubiquiti M-series device, makes unauthorized copies of and modifies the configuration portion of Ubiquiti's firmware present on Ubiquiti M-series devices in violation of the Ubiquiti Firmware License Agreements.

74. The Hacked Firmware, when installed by Cambium, a Cambium distributor or a Ubiquiti customer on a Ubiquiti M-series device, deletes the Ubiquiti kernel, including Ubiquiti radio control software, and the AIRMAX® technology platform on Ubiquiti M-series devices, in violation of the Ubiquiti Firmware License Agreements.

75. The Hacked Firmware, when installed by Cambium, a Cambium distributor or a Ubiquiti customer on a Ubiquiti M-series device, deletes the Ubiquiti file system software on Ubiquiti M-series devices in violation of the Ubiquiti Firmware License Agreements.

76. As described herein, the Hacked Firmware preserves other portions of the Ubiquiti firmware present on M-series devices and makes unauthorized use of the Ubiquiti firmware after the Hacked Firmware is installed and running on Ubiquiti M-series devices.

77. The Hacked Firmware, when installed by Cambium, a Cambium distributor or a Ubiquiti customer on a Ubiquiti M-series device, preserves and makes unauthorized use of Ubiquiti's binary, proprietary calibration portion of the firmware present on the Ubiquiti M-series devices in violation of the Ubiquiti Firmware License Agreements.

78. As described herein, the Hacked Firmware, when installed by Cambium, a Cambium distributor or a Ubiquiti customer on a Ubiquiti M-series device, deletes and replaces the user interfaces on Ubiquiti M-series devices with a completely different, hacked user interface in violation of the Ubiquiti Firmware License Agreements.

79. The Hacked Firmware when installed by Cambium, a Cambium distributor or a Ubiquiti customer on a Ubiquiti M-series device eliminates all Ubiquiti copyright notices from the user interface on M-series devices, in violation of the Ubiquiti Firmware License Agreements.

80. The Hacked Firmware when installed by Cambium, a Cambium distributor or a Ubiquiti customer on a Ubiquiti M-series device replaces Ubiquiti copyright notices in a hacked user interface on M-series devices with Cambium copyright notices, notwithstanding the presence of Ubiquiti firmware on the hacked device.

81. The Hacked Firmware when installed by Cambium, a Cambium distributor or a Ubiquiti customer on a Ubiquiti M-series device includes Ubiquiti trademarks in the hacked user interface.

82. The Hacked Firmware, when installed by Cambium, a Cambium distributor or a Ubiquiti customer on a Ubiquiti M-series device, completely replaces the radio software and

thereafter permits the entry of radio transmission values through the hacked user interface that exceed radio restrictions implemented on the M-series devices and defeats Ubiquiti radio controls all in violation of the Ubiquiti Firmware License Agreement and FCC Rules and Regulations.

83. Cambium intentionally misleads and induces distributors and Ubiquiti customers to willfully and intentionally breach Ubiquiti's copyrights in its firmware by making unauthorized copies of copyrighted portions of Ubiquiti's firmware and by copying, installing or re-installing copies Ubiquiti's copyrighted firmware on M-series devices without authorization for the sole purpose of facilitating the hacking of Ubiquiti M-series devices by installing or reinstalling the Hacked Firmware.

84. Cambium's Hacked Firmware is a product of unauthorized reverse engineering of the Ubiquiti firmware stored on M-series devices and incorporates features capable of circumventing Ubiquiti's access control mechanisms, including mechanisms used to verify firmware as permissible on M-series devices.

85. The Hacked Firmware includes replacement radio software that changes the radio of M-series devices such that operation of the modified devices is impermissible under the FCC's Rules and Regulations.

86. Cambium traffics in Hacked Firmware that it directs distributors and Ubiquiti customers to install on Ubiquiti M-series devices to circumvent the access control protection mechanisms of the Ubiquiti firmware. This allows the Hacked Firmware to copy and gain unauthorized access to proprietary calibration and configuration information preserved on the M-series devices after the hacking.

87. Cambium's Hacked Firmware thereafter changes the radio on Ubiquiti M-series devices and causes the Ubiquiti M-series devices to transmit at power levels and with frequencies that violate FCC rules and equipment authorizations.

88. In early 2017, Ubiquiti introduced "signed" versions of the Ubiquiti AirOS firmware on newly produced M-series devices, and made these signed versions available for download for M-series devices, including AirOS firmware versions 5.6.15 and 6.0.3. These firmware versions are more difficult to hack than prior versions. Yet, Cambium has provided its end users with instructions on ways to attempt to hack the signed AirOS firmware versions.

89. Cambium traffics in Hacked Firmware and instructions to Ubiquiti customers that circumvent additional access controls on signed versions of Ubiquiti firmware for M-series devices. Cambium's instructions are premised on intentional, unauthorized copying of copyrighted Ubiquiti firmware in order to defeat the signed versions of Ubiquiti firmware for M-series devices, followed by additional hacking of the Ubiquiti M-series devices with the Hacked Firmware to circumvent access control mechanisms within the Ubiquiti firmware, and copy and gain unauthorized access to proprietary calibration and configuration information preserved on the M-series devices after the hacking.

90. Cambium's promotion of and trafficking in Hacked firmware is willful, wanton, fraudulent, and has been deliberately designed and carried out to damage Ubiquiti's customer relationships, unfairly compete with Ubiquiti and migrate Ubiquiti customers to Cambium customers.

91. Cambium and those distributors, customers and other agents that Cambium has misled and induced to commit willful breaches and violations of the Ubiquiti Firmware License Agreements described herein each exceeded the limited, authorized access that Ubiquiti provides

to use the firmware on Ubiquiti M-series devices. As a result, Cambium and/or its agents hacking of the Ubiquiti firmware in Ubiquiti M-series devices in furtherance of creating the Hacked Firmware immediately and automatically terminated the Ubiquiti Firmware License Agreements for Cambium and/or its agents. Cambium's and/or its agents intentional and willful acts to access and continue to access protected devices, Ubiquiti M-series devices and Ubiquiti websites used in interstate commerce and communications, to hack, copy, modify, remove, and make unauthorized use of Ubiquiti's firmware and M-series devices were all without authorization and in violation of the Computer Fraud and Abuse Act and the Illinois Computer Crime Prevention Law.

92. Cambium has provided information and firmware to facilitate users switching from signed AirOS firmware versions to the Hacked Firmware. *See* Postings on Cambium Community Forum, Exhibit K.

Cambium's False and Misleading Statements to Promote the Hacked Firmware

93. On and around November 30, 2016, Cambium made announcements on its website and released a webinar announcing the general availability of the Hacked Firmware as a replacement for Ubiquiti's native firmware. The lead speakers during the webinar were Defendants Sakid Ahmed and Dmitry Moiseev. The webinar directs viewers to the Cambium website to download the Hacked Firmware and provides instructions on how to navigate the Ubiquiti web user interfaces driven by Ubiquiti firmware on M-series Ubiquiti devices in order to replace the Ubiquiti firmware with Cambium's Hacked Firmware.

94. During the webinar Defendants Ahmed and Moiseev—Cambium representatives—directly targeted Ubiquiti customers—claiming that the Hacked Firmware would "support . . . XW-based Ubiquiti hardware (2013-current) [,and] XM-based Ubiquiti hardware (2013 and prior)" totaling 17 supported Ubiquiti models.

95. During the webinar, Defendants Ahmed and Moiseev touted that Cambium would "continue to develop ePMP Elevate" in order to provide "[s]upport for more Ubiquiti subscriber modules."

96. During the webinar, Defendants Ahmed and Moiseev also held a live demonstration providing step-by-step instructions to Ubiquiti customers on how to install the Hacked Firmware. Defendants Ahmed and Moiseev demonstrated in real time Cambium's improper hacking of the Ubiquiti product.

97. During the webinar, Cambium also showed its so-called "lab" wherein Cambium had on display the Ubiquiti M-series devices.

98. During the webinar, Defendants Ahmed and Moiseev answered nearly a dozen live questions from the audience specifically regarding Ubiquiti, including pertaining to the alteration of Ubiquiti hardware and the supposed ability to reverse changes made to the Ubiquiti firmware through installation of the Hacked Firmware.

99. During the webinar, Defendants Ahmed and Moiseev referred customers with warranty questions to the hardware manufacturers, which include Ubiquiti.

100. The webinar was conducted by Defendant Sakid Ahmed, Vice President of Engineering, along with Cambium employees involved in product design and development for the Hacked Firmware, including Dmitry Moiseev.

101. Defendants Ahmed and Moiseev's statements to the public implied that Ubiquiti endorsed the Hacked Firmware—a false and misleading fact.

102. Cambium and its representatives have made numerous misrepresentations during the webinar.

103. For instance, during the webinar, Cambium representatives stated that "Once you've uploaded ePMP Elevate . . . old manufacturers' firmware is not operating in any form." (Exhibit F), Webinar, at 49:56-50:03. This is false. Various parameters and other portions of the Ubiquiti M-series firmware code remain operative after the Hacked Firmware is installed.

104. There were also numerous false statements by omission made during the webinar.

105. For instance, Cambium never disclosed during the webinar or in any promotional materials for the Hacked Firmware the following critical facts:

- that use of the ePMP Elevate Software violates the terms of the Ubiquiti licensing agreements;
- that the changes made with the Cambium Firmware alters the device to be non-FCC compliant;
- that use of the ePMP Elevate Software violates the licensing terms, which also voids the warranty; and
- that use of the ePMP Elevate Software infringes Ubiquiti's intellectual property.

106. The individual Defendants routinely have publicly touted the purported benefits of the Hacked Firmware in an effort to attract Ubiquiti customers.

107. So too has Cambium Network's President and Chief Executive Officer, Atul Bhatnagar, who was quoted in a December 7, 2016 article and a November 30, 2016 blog post on the Cambium Website touting the purported benefits of the Hacking ePMP Elevate Firmware. *See* https://appdevelopermagazine.com/4690/2016/12/7/cambium-networks-jailbreaks-first-wireless-broadband-network/ (quoting Mr. Bhatnagar as emphasizing the fact that ePMP Elevate is compatible with various types of hardware: "ePMP Elevate is a software solution that is hardware agnostic[.]" "Network operators with radio hardware from one or multiple vendors can now operate one network with a common management system without replacing installed CPE hardware."); *see also* https://www.cambiumnetworks.com/blog/cambium-networks-announces-

new-epmp-elevate-platform-adding-new-capabilities-to-existing-wireless-broadband-networks/ (stating same).

108. Cambium promoted its Quick Start Guide during its November 30, 2016 webinar targeting Ubiquiti customers stating that Cambium "strongly recommends" viewers read the Quick Start Guide.

109. On information and belief, on or about November 30, 2016, Cambium released an ePMP Portfolio Overview, which identifies the Hacked Firmware as a product called "elevate" and uses the Ubiquiti trademark to refer to the devices on which Cambium's Hacked Firmware should be installed.

110. On information and belief, on or around November 30, 2016, Cambium released a Quick Start Guide instructing Ubiquiti customers on steps to download the Hacked Firmware from the Cambium website and install it through the web user interfaces driven by Ubiquiti firmware on M-series devices. The Quick Start Guide contained numerous material misrepresentations.

111. For instance, in its Quick Start Guide, Cambium stated that "[a]fter the upgrade, the ePMP Elevate subscribers retain only their configured IP Address and Device Name. All other parameters, including configured access points SSIDs, frequency configuration, VLAN, etc. may be configured over-the-air after upgrade to ePMP Elevate." ePMP Elevate Quick Start Guide v3.2 (Nov. 2016) (Ex. D) at pg. 5. This statement is literally false. Multiple Ubiquiti parameters are copied, maintained, and used by ePMP Elevate, the Hacked Firmware.

112. Cambium also made misleading and/or false representations in its Quick Start Guide regarding the impact of the Hacked Firmware on FCC Standards:

> FCC Standards:
>
> Caution! The user must ensure that deployed ePMP products operate in accordance to local regulatory limits. ePMP and ePMP

> Elevate-compatible devices may not share regulatory certifications in all regions.
>
> Some 3rd-party radio devices were originally FCC-certified and labeled to operate in the 5.8 GHz frequency range only. An ePMP Elevate upgrade enables 3rd-party radios to operate within the U-NII-1 through U-NII-4 frequency band range 5150 – 5980 MHz. To ensure FCC regulatory compliance for ePMP Elevate-upgraded radio devices:
>
> 1. A **new label must be applied** to the device with the updated FCC ID clearly visible. 3rd-party radio manufacturers support FCC label requests online (labels are shipped directly).
>
> 2. FCC-allowed transmit power in the 5.8 GHz band has been reduced with the latest regulatory guidelines. **ePMP Elevate adheres to these FCC power limits**, and an upgrade to ePMP Elevate software **may introduce a reduction of the device's operating transmit power to adhere to regulatory limits** (as a result of the ePMP access point's transmit power control mechanism).

ePMP Elevate Quick Start Guide v3.2 (Nov. 2016) (Ex. D) at pg. 2 (emphasis added).

113. These statements regarding compliance with FCC standards are false and/or misleading. The statement that "a reduction of the device's operating transmit power" may "adhere to regulatory limits" is false and/or misleading. These statements imply customers can comply with FCC standards using the Hacked Firmware on Ubiquiti's M-series devices, when this is inaccurate.

114. On information and belief, Cambium's promotion of its Hacked Firmware to Ubiquiti customers with Ubiquiti M-series devices contains false and misleading information about the nature of the Hacked Firmware and its impact after installation on Ubiquiti M-series devices.

115. On information and belief, Cambium promotes the Hacked Firmware, for example, by falsely stating that after installing the Hacked Firmware on a Ubiquiti M-series device the original firmware is no longer present or operating in any form.

116. On information and belief, Cambium also falsely promotes the Hacked Firmware to Ubiquiti customers by stating that the original device manufacturer provides a hardware warranty for the Ubiquiti M-series devices that have been hacked by the installation of Cambium's Hacked Firmware.

117. On information and belief, Cambium also falsely and misleadingly promotes the installation and use of Hacked Firmware to Ubiquiti customers with Ubiquiti M-series devices by stating that after hacking Ubiquiti M-series devices by installing Cambium's Hacked Firmware, that the hacker can ensure FCC compliance by having a third party manufacturer, who is not the source of the Hacked Firmware, generate and apply a new FCC label to the device.

118. On information and belief, Cambium's false and misleading promotion of the Hacked Firmware for use with Ubiquiti M-series devices was carried out in order to capitalize on the goodwill and brand recognition that Ubiquiti developed—through the investment of resources—in the marketplace Cambium directly targeted existing Ubiquiti customers in an effort to damage these customers' brand loyalty and recognition of the Ubiquiti name and high quality standards associated therewith.

119. On information and belief, Cambium's false and misleading promotion of the Hacked Firmware for use with Ubiquiti M-series devices was carried out for commercial reasons to sell new Cambium access points with which to interface a customer's installed base of Ubiquiti M-series products after those Ubiquiti M-series products have been hacked with the Hacked Firmware.

120. Cambium's website contains a "Community" forum where members of the public—including potential and current Ubiquiti customers—may post questions and comments.

121. During its November 30, 2016 webinar, Cambium encouraged listeners to use the Cambium Community forum, noting that its employees were "active" users of the Community forum.

122. Cambium personnel, posting under a Cambium account displaying the Cambium logo, frequently post on the Community.Cambiumnetworks.com website on various message boards.

123. Numerous of the message boards directly target Ubiquiti customers by referencing and commenting on Ubiquiti products.

124. On one message board thread entitled "Ubiquiti LB23 does not respond after installing Elevate", Luis—who is identified on the board as a Cambium Employee—responded to provide the customer advice on altering the Hacked Firmware. This demonstrates Cambium's direct efforts to target and interfere with Ubiquiti's relationships with its existing customers.

125. On one message board thread entitled "Turning UBNT to ePMP Subscribers" a Cambium employee, Defendant Sakid Ahmed—who was identified as the "Moderator" of the board—posted statements regarding Cambium's supposed power performance in order to encourage customer to install the Cambium Hacked Firmware.

126. In a post dated December 25, 2017, Defendant Dmitry—noted as an "occasional contributor"—posted on a message board instructing a user on how to use ePMP with Ubiquiti power supplies.

Cambium's Instructions to Ubiquiti Customers Induce Breach of the Ubiquiti Firmware License Agreements and Installation of the Hacked Firmware

127. Cambium's promotional videos and Quick Start Guide, among other forms of promotion, instruct Ubiquiti customers to install the Hacked Firmware on their Ubiquiti M-series devices through the Ubiquiti M-series web interface. In some cases, Cambium instructs Ubiquiti

customers to download and install certain versions of Ubiquiti firmware prior to hacking a Ubiquiti M-series device by installing the Cambium Hacked Firmware.

128. The Ubiquiti M-series devices and the use of Ubiquiti firmware on the M-series devices are covered by Ubiquiti Firmware License Agreements.

129. In addition to Cambium's own breaches of Ubiquiti license Agreement by creating, using and distributing the Hacked Firmware, Cambium's instructions to Ubiquiti customers to hack the Ubiquiti M-series devices by installing the Hacked Firmware causes the customer to breach the Ubiquiti license agreements and is a further breach by Cambium.

130. Cambium's use of Ubiquiti's name and trademarks in promotion conveys that manufactures like Ubiquiti will honor hardware warranties after hacked firmware is installed by a customer. On information and belief, Cambium's statements that no firmware from Ubiquiti remains on the Ubiquiti device after installation, and that obtaining an FCC label from a third party manufacturer will ensure FCC compliance are all intentional, calculated, false and/or unauthorized statements by Cambium, who as a manufacturer of similar hardware, should know better. These calculated misrepresentations and unauthorized uses of Ubiquiti's name and trademarks deliberately aim to deceive and induce customers into hacking their existing installed base of Ubiquiti M-series devices with Cambium's Hacked Firmware for the purpose of selling more Cambium access points and hardware and migrating Ubiquiti customers to Cambium hardware.

The Hacking Enterprise and Its Racketeering Activity

131. Cambium sits at the helm of the Hacking Enterprise—an association-in-fact—consisting of Cambium, Cambium Networks, Sakid Ahmed, Dmitry Moiseev, and distributor Winncom. At all relevant times, the Hacking Enterprise constituted an association-in-fact enterprise within the meaning of 18 U.S.C. §§ 1961(4) and 1962(c).

132. At all relevant times, the Hacking Enterprise was engaged in interstate and international commerce and involved in activities affecting interstate and international commerce.

133. Although functioning as independent legal entities, Cambium, Cambium Networks, and Winncom joined together with Defendants Moiseev and Ahmed for the common purpose of ensuring financial gain for themselves through misleading Ubiquiti customers.

134. The purpose of the Hacking Enterprise was to carry out a scheme to obtain money by persuading Ubiquiti customers to leave for Cambium based on material misrepresentations and omission, and sell Cambium equipment by competing unfairly against Ubiquiti.

135. Cambium led this Hacking Enterprise, with Winncom and Defendants Moiseev and Ahmed assisting in attracting customers.

136. Cambium Networks helped fund the Hacking Enterprise, by providing monetary support to Cambium and having Cambium carry out all distribution to Winncom in the United States.

137. Defendants Ahmed and Moiseev marketed the Hacked Firmware to the public through promotional and instructional videos and, on information and belief, designed the Hacked Firmware.

138. The members of the Hacked Enterprise came together with the specific purpose of ensuring financial gain via misleading and inducing consumers to purchase and install the Hacked Firmware among other illicit business and profit gaining purposes. On information and belief, the members of the Hacking Enterprise exchanged numerous emails, phone calls, and communications to strategize regarding the launch of the Hacked Firmware and the best ways to attract Ubiquiti customers and ensure commercial success of the Hacked Firmware and attraction and long-term success of the Hacked Firmware.

139. Each member of the Hacking Enterprise was recruited by Cambium, and Cambium provided each member of the Hacking Enterprise financial incentives and/or direct financial benefit for participation in the Hacking Enterprise.

140. The Hacking Enterprise carried out its goal of ensuring financial gain by engaging in various acts of willful copyright infringement and mail and wire fraud to induce customers to partially remove Ubiquiti firmware by installing the Hacked Firmware, copying portions of the Ubiquiti firmware, and circumventing signed versions of Ubiquiti firmware without authorization to ensure that Ubiquiti M-series devices would no longer be compatible with a Ubiquiti network using Ubiquiti protocols and would instead be used with newly purchased Cambium networking equipment compatible with the Hacked Firmware.

141. The Hacking Enterprise trafficked in and made material misrepresentations and omissions regarding the Hacked Firmware specifically to defraud and induce end users and customers into breaching the Firmware License Agreement and to make changes to the Ubiquiti M-series device.

142. The scheme of the Hacking Enterprise has been going on since at least November 30, 2016, at which point in time Cambium, with the knowledge and encouragement of its parent corporation Cambium Networks and through its Vice President of Engineering Sakid Ahmed, as well as employee Dmitry Moiseev, in conjunction Winncom, began promoting the Hacked Firmware and offering it for sale on the internet to consumers.

143. The Hacking Enterprise carried out its goal of obtaining financial gain at the expense of customers and Ubiquiti through a pattern of racketeering activity.

144. First, the Hacking Enterprise members conspired together to concoct a scheme to mislead and induce customers to purchase and install the Hacked Firmware.

145. The scheme began with Cambium, working with the funding and encouragement of its parent Cambium Networks, entering into partnerships with Blip and Winncom to traffic in and promote the Hacked Firmware.

146. On information and belief, in exchange for offering positive statements regarding the use of the Hacked Firmware, Blip and Winncom were able to take advantage of Cambium's special discount offered to customers that "spread the word" regarding the Hacked Firmware.

147. The Hacking Enterprise accomplished its promotion of the Hacked Firmware and inducement of third-party purchases and installation in various ways.

148. For instance, Blip and the Hacking Enterprise conspired together to issue various public comments regarding purported benefits that Blip gained from installation of the Hacked Firmware.

149. On November 29, 2016, Cambium posted on its website a "Resource" which touted that Blip's use of the Hacked Firmware "dramatically improved performance."

150. Cambium also quoted from co-conspirator Blip's co-owner, Ian Ellison, in product release announcements that touted the benefits of the Hacked Firmware.

151. Cambium's citation to the benefits Blip purportedly incurred in using the Hacked Firmware was done in order to specifically target customers of Ubiquiti. And, on information and belief, the members of the Hacking Enterprise were all aware of Cambium's intent to advertise the purported benefits to Blip from using the Hacked Firmware.

152. Winncom posted on its website numerous advertisements touting the supposed benefits of the Hacked Firmware, including seven separate "EPMP Case Studies" describing the Hacked Firmware.

153. Winncom has held seminars for Cambium—in an effort to assist the Hacking Enterprise—at its goal of attracting customers. One such seminar, which included a product demonstration of the Hacked Firmware was held on October 7, 2017 at a WISPApalooza event.

154. Sakid Ahmed and Dmitry Moiseev attended the WISPApalooza event on behalf of Cambium in an effort to work with Winncom to spread false and misleading information regarding the Hacked Firmware and to lure away Ubiquiti customers.

155. Winncom also served as a "Connected Partner" for Cambium, receiving various benefits to "reward" Winncom for furthering the Hacking Enterprise's scheme.

156. On February 17, 2012, Cambium Networks posted on its website, a press release touting a new "Connected Partner Program" of which Winncom was a partner distributor.

157. Winncom's advertisement of the case studies discussing the Hacked Firmware was done in order to specifically target Ubiquiti customers and induce purchases and use of the Hacked Firmware.

158. The Hacking Enterprises' misleading advertisements and tutorials were provided to consumers to mislead them and induce them to install the Hacked Firmware on Ubiquiti M-series devices, notwithstanding that doing so would violate FCC rules and the Ubiquiti Firmware License Agreements, in order to damage Ubiquiti M-series devices and their licensed firmware by rendering them unable to communicate with other Ubiquiti devices using Ubiquiti protocols, and in order for Cambium to sell Cambium equipment with which the newly installed Hacked Firmware on Ubiquiti M-series devices is compatible.

159. Ubiquiti has been directly and proximately harmed by the Hacking Enterprises' false advertisements and statements because customers are misled and induced to violate Ubiquiti

Firmware License Agreements, Ubiquiti intellectual property rights and FCC rules by hacking the Ubiquiti product they purchased with the Hacked Firmware.

160. Although the full extent of wire and mail fraud carried out by the Hacking Enterprise in furtherance of their scheme to mislead consumers and sell the Hacked Firmware remains to be determined, the following are examples of fraudulent statements members of the Hacked Enterprise made using the U.S. Mail and/or interstate wires:

- The Cambium website's advertisement of a "Resource Guide" which discusses purported benefits Blip gained from installation of the Hacked Firmware, without disclosing the true nature of the Hacked Firmware.
- Cambium's running of "field experience" webinars wherein Cambium discussed Blip's experience using the Hacked Software, without disclosing the true nature of the Hacked Firmware.
- Cambium's launching and showing of various promotional videos on its website that discuss purported "benefits" of the Hacked Firmware and instruct Cambium Customers to install the Hacked Firmware on their Ubiquiti M-series devices through the Ubiquiti M-series web interface, without disclosing the true nature of the Hacked Firmware.
- Cambium's issuance of a press release on November 30, 2016 touting the Hacked Firmware's benefit and Blip's experience, without disclosing the true nature of the Hacked Firmware.
- Cambium's November 30, 2016 webinar designed to target Ubiquiti customers and provide a step-by-step procedure for hacking the Ubiquiti M-series Firmware, which prominently featured Defendants Ahmed and Moiseev, which contained numerous material misrepresentations and omissions described in paragraphs 93-105, 108, *infra* and Exhibit F.
- Winncom's hosting of a ePMP course on October 7th-9th, 2017 at WSIPApalooza 2017—an event attended by Defendants Ahmed and Moiseev—wherein Winncom in connection with Cambium hosted a session regarding "hardware installation" which, upon information and belief, involved Winncom providing a how-to tutorial to WISPs who ultimately sold the Hacked Firmware to customers, without disclosing the true nature of the Hacked Firmware.
- Winncom's advertising campaign regarding it ePMP course at WISPApalooza in advance of the event in October 2017, which failed to disclose the true nature of the Hacked Firmware. *See* http://www.winncom.com/en/news/15358.

- Winncom's staging of a promotion via its website in the Russian language whereby licenses to Elevate were provided free of charge to potential customers to induce hacking of the Ubiquiti Firmware. Specifically, on a Winncom affiliate website, Winncom advertised that: Cambium Networks is launching a campaign to help owners of wireless networks built on Ubiquiti equipment upgrade their network by replacing old equipment with the base station of the ePMP1000 series or ePMP 2000. When purchasing new ePMP equipment, you get an Elevate license as a gift !!!" *See* http://winncom.ru/news/license-epmp-elevate (Exhibit L).

- Cambium's issuance of promotional videos and a Quick Start Guide, which instruct Cambium Customers to install the Hacked Firmware on their Ubiquiti M-series devices through the Ubiquiti M-series web interface, which failed to disclose the true nature of the Hacked Firmware. Upon information and belief, the promotional videos and Quick Start Guide were released via the Cambium website on or about November 30, 2016.

- Defendants Ahmed and Moiseev made numerous posts on Cambium's message boards disseminating false and misleading information regarding the Hacked Firmware and providing encouragement to customers installing the Hacked Firmware.

- With the knowledge and encouragement of Winncom, and Cambium Networks, Cambium hosted a video webinar featuring Defendants Ahmed and Moiseev in late 2016 wherein Cambium made false statements regarding the Hacked Firmware. These materially false statements and omissions are outlined in detail in paragraphs 93-105 of the instant Complaint.

- Cambium's publication of a Quick Start Guide containing materially false statements and omissions described herein at paragraphs 110-113 of the instant Complaint.

161. Each of these statements were made through the wires and/or the US mails with the intent to defraud and induce consumers to install the Hacked Firmware.

162. On information and belief, Cambium also used the U.S. Mail to send promotional advertisements which encouraged customers to use the Hacked Firmware on the Ubiquiti devices.

163. On information and belief, Cambium used the U.S. Mail to send invoices for the Hacked Firmware to customers throughout the United States, including in this District.

164. On information and belief, in furtherance of the Hacking Enterprise, the Hacking Enterprise members communicated with each other via e-mail communications and over the phone.

165. On information and belief, income in furtherance of the Hacking Enterprise's scheme as received via wires when customers paid on-line to purchase the Hacked Firmware.

166. The advertisements, promotions, and web videos on the Cambium site were broadcast to and viewed by consumers throughout the United States.

167. The advertisements on the Winncom website was viewed and transmitting via the wires to consumers throughout the United States.

FIRST CLAIM FOR RELIEF
(Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030)
(Asserted Against Cambium)

168. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

A. CFAA § 1030(a)(2)(C) Violations

169. Section 1030(a)(2)(C) of the CFAA prohibits a person from intentionally accessing a protected computer without or in excess of authorization and obtaining information from a protected computer.

170. Ubiquiti's M-series devices are protected computers within the meaning of the CFAA because the M-series devices are used in and affect interstate commerce.

171. Cambium has itself, and has aided and abetted others, to intentionally install the Hacked Firmware on Ubiquiti M-series devices in violation of multiple provisions of the Ubiquiti Firmware License Agreements, and by so doing makes unauthorized access to among other things, Ubiquiti M-series devices and licensed firmware including configuration and calibration

information on the Ubiquiti M-series devices (the protected computers) in order to damage and take control of the Ubiquiti M-series devices for Cambium's commercial purposes.

172. By virtue of this conduct, Cambium has violated and has conspired with others to violate the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(C), by intentionally accessing Ubiquiti M-series devices, which consist of protected computers used for interstate commerce or communications, without authorization or by exceeding authorized access to the Ubiquiti M-series devices, and by accessing configuration and calibration information in order to take control of the Ubiquiti M-series devices for Cambium's commercial purposes.

173. Ubiquiti has sustained damage and loss by, *inter alia*, having the Ubiquiti Firmware, which underlies its Firmware License Agreements with customers of Ubiquiti M-series devices, impaired and altered and no longer compatible with other Ubiquiti devices using Ubiquiti's wireless protocols.

174. Cambium's Hacked Firmware has been provided by Cambium and third parties authorized by Cambium to well in excess of ten (10) Ubiquiti M-series devices, which are protected computers.

175. Ubiquiti has spent in excess of $100,000 investigating the nature of the Hacked Firmware and the damage it causes to Ubiquiti Firmware on Ubiquiti M-series devices resulting from Cambium's wrongful conduct.

176. Ubiquiti is entitled to damages for Cambium's violation of Section 1030(a)(2)(C) of the CFAA in an amount to be determined at trial.

177. Unless restrained and enjoined, Cambium will continue to commit such acts. Ubiquiti's remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Ubiquiti to remedies, including injunctive relief, as provided by 18 U.S.C. § 1030(g).

B. CFAA § 1030(a)(4) Violations

178. Section 1030(a)(4) of the CFAA prohibits a person from knowingly, and with intent to defraud, accessing a protected computer without authorization or in excess of authorized access and by means of such conduct furthering the intended fraud and obtaining anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period.

179. Ubiquiti's M-series devices are protected computers within the meaning of the CFAA because the M-series devices are used in and affect interstate commerce.

180. Cambium developed the Hacked Firmware intentionally and to perform hacks of Ubiquiti M-series devices that violate the Ubiquiti Firmware License Agreements in multiple ways, including removing copyrighted portions and copying copyrighted portions all during unauthorized access and installation of the Hacked Firmware on a protected computer, the Ubiquiti M-series device.

181. Cambium itself and by conspiring with others has intentionally defrauded Ubiquiti customers, including with misrepresentations by Cambium as to the nature of the Hacked Firmware, into breaching the Ubiquiti Firmware License Agreements and hacking their Ubiquiti M-series devices in furtherance of Cambium's profit making scheme.

182. Cambium's above described conduct has resulted in loss and damage to Ubiquiti's reputation and by having the Ubiquiti Firmware, which underlies its Firmware License Agreements with customers of Ubiquiti M-series devices, impaired and altered and no longer compatible with other Ubiquiti devices using Ubiquiti's wireless protocols, all of which greatly exceeds $5,000.

183. Indeed, on information and belief, the Hacked Firmware has been installed on hundreds of Ubiquiti M-series devices in the United States alone and Cambium itself charges an annual "license" fee of $35 per year for each installation of Hacked Firmware.

184. The configuration information and binary data obtained by Cambium from each unauthorized access to a Ubiquiti M-series device, and the impairment of the Ubiquiti firmware on those devices which render the M-series devices inoperable with other Ubiquiti devices using Ubiquiti protocols, is a scheme to defraud Ubiquiti and its customers that consists of more than the mere use of Ubiquiti M-series devices.

185. By its above described conduct, Cambium has violated § 1030(a)(4) of the CFAA, by knowingly and with intent to defraud, accessing Ubiquiti M-series devices, which consist of protected computers used for interstate commerce or communications, without authorization, or by exceeding their authorized access, and by means of such access furthering the intended fraud and obtaining configuration information and binary data necessary to operate each M-series device.

186. Ubiquiti has sustained damage and loss by, *inter alia*, having the Ubiquiti Firmware which underlies its Firmware License Agreements with customers impaired and altered and no longer compatible with other Ubiquiti devices using Ubiquiti's wireless protocols.

187. Cambium's Hacked Firmware has been provided by Cambium and third parties authorized by Cambium to well in excess of ten (10) Ubiquiti M-series devices, which are protected computers.

188. Ubiquiti has spent in excess of $100,000 investigating the nature of the Hacked Firmware and the damage it causes to Ubiquiti Firmware on Ubiquiti M-series devices resulting from Cambium's wrongful conduct

189. Ubiquiti is entitled to damages for Cambium's violation of § 1030(a)(4) of the CFAA in an amount to be determined at trial.

190. Unless restrained and enjoined, Cambium will continue to commit such acts. Ubiquiti's remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Ubiquiti to remedies, including injunctive relief, or other equitable relief, as provided by 18 U.S.C. § 1030(g).

C. CFAA § 1030(a)(5)(A) Violations

191. Section 1030(a)(5)(A) of the CFAA prohibits knowingly causing the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causing damage without authorization, to a protected computer.

192. Ubiquiti's M-series devices are protected computers within the meaning of the CFAA because the M-series devices are used in and affect interstate commerce.

193. Cambium transmits and aids and abets third parties, including Ubiquiti's customers in the installation of the Hacked Firmware on Ubiquiti M-series devices in violation of the access restrictions pursuant to Ubiquiti Firmware License Agreements, causing damage to the Ubiquiti M-series devices including the removal of large portions of the Ubiquiti firmware, which results in the Ubiquiti M-series devices being impaired and no longer able to connect to other Ubiquiti devices using Ubiquiti's wireless protocols. The code and information transmitted cause the unauthorized access and the damage to Ubiquiti and the Ubiquiti M-series devices.

194. Cambium's Hacked Firmware directly and intentionally damages Ubiquiti and the Ubiquiti M-series devices. It alters the code on these devices and changes the composition of these devices in direct violation of the governing Ubiquiti Firmware Licensing Agreements.

195. By its above described conduct, Cambium has violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(A), by knowingly causing the transmission of a program,

information, code or command, including causing the transmission of the Hacked Firmware, and as a result of such conduct, intentionally causing damage without authorization to a protected computer.

196. Ubiquiti has sustained damage and loss by, *inter alia*, having the Ubiquiti Firmware, which underlies its Firmware License Agreements with customers, impaired and altered and no longer compatible with other Ubiquiti devices using Ubiquiti's wireless protocols.

197. Cambium's Hacked Firmware has been provided by Cambium and third parties authorized by Cambium to well in excess of ten (10) Ubiquiti M-series devices, which are protected computers.

198. Ubiquiti has spent in excess of $100,000 investigating the nature of the Hacked Firmware and the damage it causes to Ubiquiti Firmware on Ubiquiti M-series devices resulting from Cambium's wrongful conduct.

199. Accordingly, Ubiquiti is entitled to damages for Cambium's violation of Section 1030(a)(5)(A) of the CFAA in an amount to be determined at trial.

200. Unless restrained and enjoined, Cambium will continue to commit such acts. Ubiquiti's remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Ubiquiti to remedies, including injunctive relief, and other equitable relief, as provided by 18 U.S.C. § 1030(g).

D. CFAA § 1030(a)(5)(B) Violations

201. Section 1030(a)(5)(B) of the CFAA prohibits a person from intentionally accessing a protected computer without authorization, and as a result of such conduct, recklessly causing damage.

202. Ubiquiti's M-series devices are protected computers within the meaning of the CFAA because the M-series devices are used in and affect interstate commerce.

203. Cambium transmits and aids and abets third parties, including Ubiquiti's customers in the installation of the Hacked Firmware on Ubiquiti M-series devices in violation of the access restrictions pursuant to Ubiquiti Firmware License Agreements, causing damage to the Ubiquiti M-series devices including the removal of large portions of the Ubiquiti Firmware, which results in the Ubiquiti M-series devices being impaired and no longer able to connect to other Ubiquiti devices using Ubiquiti's wireless protocols. The code and information transmitted cause the unauthorized access and the damage to Ubiquiti and the Ubiquiti M-series devices.

204. Cambium's conduct is intentional, and its Hacked Firmware recklessly, and with full knowledge of Cambium, causes the damage to the Ubiquiti M-series devices described above in direct violation of the governing Ubiquiti Firmware Licensing Agreements.

205. Cambium intentionally ignores the restrictions set forth in the Ubiquiti Firmware Licensing Agreements with malice and disregard, demonstrating its reckless behavior in transmitting and aiding and abetting third parties, including Ubiquiti's customers, in the installation of the Hacked Firmware on Ubiquiti M-series devices in violation of the access restrictions pursuant to License Agreements.

206. Thus, Cambium has violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(B), by intentionally accessing one or more M-series devices, which consist of protected computers, without authorization, and as a result of such conduct, recklessly causing damage.

207. Ubiquiti has sustained damage and loss by, *inter alia*, having the Ubiquiti Firmware, which underlies its Firmware License Agreements with customers, impaired and altered and no longer compatible with other Ubiquiti devices using Ubiquiti's wireless protocols.

208. Cambium's Hacked Firmware has been provided by Cambium and third parties authorized by Cambium to well in excess of ten (10) Ubiquiti M-series devices, which are protected computers.

209. Ubiquiti has spent in excess of $100,000 investigating the nature of the Hacked Firmware and the damage it causes to Ubiquiti Firmware on Ubiquiti M-series devices resulting from Cambium's wrongful conduct.

210. Accordingly, Ubiquiti is entitled to damages for Cambium's violation of Section 1030(a)(5)(B) of the CFAA in an amount to be determined at trial.

211. Unless restrained and enjoined, Cambium will continue to commit such acts. Ubiquiti's remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Ubiquiti to remedies, including injunctive relief, or other equitable relief, as provided by 18 U.S.C. § 1030(g).

E. CFAA § 1030(a)(5)(C) Violations

212. Section 1030(a)(5)(C) of the CFAA prohibits a person from intentionally accessing a protected computer without authorization, and as a result of such conduct, causing damage and loss.

213. Ubiquiti's M-series devices are protected computers within the meaning of the CFAA because the M-series devices are used in and affect interstate commerce.

214. Cambium transmits and aids and abets third parties, including Ubiquiti's customers in the installation of the Hacked Firmware on Ubiquiti M-series devices in violation of the access restrictions pursuant to Ubiquiti Firmware License Agreements, causing damage to the Ubiquiti M-series devices including the removal of large portions of the Ubiquiti Firmware, which results in the Ubiquiti M-series devices being impaired and altered and no longer able to connect to other

Ubiquiti devices using Ubiquiti's wireless protocols. The code and information transmitted cause the unauthorized access and the damage to Ubiquiti and the Ubiquiti M-series devices.

215. Cambium intentionally developed the Hacked Firmware to directly damage Ubiquiti and the Ubiquiti M-series devices for commercial advantage. It removes and alters firmware code on these devices and changes the composition of these devices in direct violation of multiple provisions of the governing Ubiquiti Firmware Licensing Agreements.

216. Thus, Cambium has violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(C), by intentionally accessing one or more M-series devices, which consist of protected computers, and, as a result of the intentional access causing the damage and loss described herein.

217. Ubiquiti has sustained damage and loss by, *inter alia*, having the Ubiquiti Firmware, which underlies its Firmware License Agreements with customers, impaired and altered and no longer compatible with other Ubiquiti devices using Ubiquiti's wireless protocols.

218. Cambium's Hacked Firmware has been provided by Cambium and third parties authorized by Cambium to well in excess of ten (10) Ubiquiti M-series devices, which are protected computers.

219. Ubiquiti has spent in excess of $100,000 investigating the nature of the Hacked Firmware and the damage it causes to Ubiquiti Firmware on Ubiquiti M-series devices resulting from Cambium's wrongful conduct.

220. Accordingly, Ubiquiti is entitled to damages for Cambium's violation of Section 1030(a)(5)(C) of the CFAA in an amount to be determined at trial.

221. Unless restrained and enjoined, Cambium will continue to commit such acts. Ubiquiti's remedy at law is not adequate to compensate it for these inflicted and threatened injuries,

entitling Ubiquiti to remedies, including injunctive relief, or other equitable relief, as provided by 18 U.S.C. § 1030(g).

F. CFAA § 1030(a)(6)(A) Violations

222. Section 1030(a)(6)(A) of the CFAA prohibits a person from knowingly and with intent to defraud trafficking in any password or similar information through which a protected computer may be accessed without authorization, if such trafficking affects interstate or foreign commerce.

223. Cambium traffics in—sells and transports to customers and third-party sellers—the Hacked Firmware and additional programs, videos and guides instructing third parties how to hack and gain unauthorized access to Ubiquiti M-series devices.

224. Through the Hacked Firmware and additional materials, consumers learn how and are able to hack and gain unauthorized access to Ubiquiti's M-series Devices.

225. The Hacked Firmware and alteration of the M-series Devices caused by installation of the Hacked Firmware, which itself facilitates unauthorized access, affects interstate commerce, as the Hacked Firmware is being distributed by Cambium and used throughout the United States and the world.

226. By the above described conduct, Cambium has violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(6)(A), by knowingly and with intent to defraud trafficking in information by distributing Hacked Firmware and additional programs, videos and guides instructing third parties how to hack and gain unauthorized access to Ubiquiti M-series devices, which trafficking and access has affected and continues to affect interstate commerce and communications and foreign commerce.

227. Ubiquiti has sustained damage and loss by, *inter alia*, having the Ubiquiti Firmware, which underlies its Firmware License Agreements with customers, impaired and altered and no longer compatible with other Ubiquiti devices using Ubiquiti's wireless protocols.

228. Cambium's Hacked Firmware has been provided by Cambium and third parties authorized by Cambium to well in excess of ten (10) Ubiquiti M-series devices, which are protected computers.

229. Ubiquiti has spent in excess of $100,000 investigating the nature of the Hacked Firmware and the damage it causes to Ubiquiti Firmware on Ubiquiti M-series devices resulting from Cambium's wrongful conduct.

230. Accordingly, Ubiquiti is entitled to damages for Cambium's violation of Section 1030(a)(6)(A) of the CFAA.

231. Unless restrained and enjoined, Cambium will continue to commit such acts. Ubiquiti's remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Ubiquiti to remedies, including injunctive relief, or other equitable relief, as provided by 18 U.S.C. § 1030(g).

G. CFAA § 1030(b)Violations

232. Section 1030(b) of the CFAA prohibits a person from conspiring to violate any other subsection of the CFAA.

233. Cambium has violated the CFAA by conspiring to commit the 18 U.S.C. § 1030(a) offenses listed above.

234. Cambium has conspired with Ubiquiti licensees of M-series device firmware to intentionally make unauthorized access by installing the Hacked Firmware, and other third parties, including Blip, who traffic in the Hacked Firmware, related software, guides and videos for

Ubiquiti M-series devices and directly or indirectly facilitate unauthorized access to the Ubiquiti M-series devices and installation of the Hacked Firmware on Ubiquiti M-series devices.

235. Ubiquiti has sustained damage and loss by, *inter alia*, having the Ubiquiti Firmware which underlies its Firmware License Agreements with customers impaired and altered and no longer compatible with other Ubiquiti devices using Ubiquiti's wireless protocols.

236. Cambium's Hacked Firmware has been provided by Cambium and third parties authorized by Cambium to well in excess of ten (10) Ubiquiti M-series devices, which are protected computers.

237. Ubiquiti has spent in excess of $100,000 investigating the nature of the Hacked Firmware and the damage it causes to Ubiquiti Firmware on Ubiquiti M-series devices resulting from Cambium's wrongful conduct.

238. Accordingly, Ubiquiti is entitled to damages for Cambium's violation of Section 1030(b) of the CFAA.

239. Unless restrained and enjoined, Cambium will continue to commit such acts. Ubiquiti's remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Ubiquiti to remedies, including injunctive relief, and other equitable relief, as provided by 18 U.S.C. § 1030(g).

H. Allegations Applicable to All CFAA Violations Asserted Herein

240. Ubiquiti has been informed and believes and thereon alleges that the actions of Cambium are knowing, deliberate, willful and in utter disregard of Ubiquiti's rights under the CFAA.

241. Ubiquiti has standing to bring the Computer Fraud and Abuse Act claims set forth above, and is entitled to remedies at law and equity pursuant to 18 U.S.C. § 1030(g) because

Cambium's conduct has caused a loss to Ubiquiti during any one (1) year period aggregating far more than $5,000 in value as specified in 18 U.S.C. § 1030(c)(4)(A)(i)(I).

242. Ubiquiti has suffered loss and has spent in excess of $100,000 investigating the Hacked Firmware in response to learning of Cambium's promotion and distribution of its Hacked Firmware to Ubiquiti M-series device customers in order to determine the nature of the Hacked Firmware and determine its response to Cambium's unauthorized access and trafficking.

243. In addition to the loss and damage to Ubiquiti, Cambium's Hacked Firmware changes the radio characteristics of the Ubiquiti M-series devices, and the Hacked Firmware exceeds radio restrictions in place on the M-series devices and that form the basis of Ubiquiti's FCC equipment authorization for the M-series devices. As modified with the Hacked Firmware, the M-series devices violate FCC rules and may constitute a threat to public safety.

SECOND CLAIM FOR RELIEF
(Violations of §§ 1201(a)(1), 1201(a)(2) and
1202(b) of the Digital Millennium Copyright Act)
(Asserted against Cambium)

244. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

A. DMCA § 1201(a)(1) Violations

245. Section 1201(a)(1) of the DMCA provides that no person shall circumvent a technological measure that effectively controls access to a work protected under this title.

246. Ubiquiti's Firmware for its M-series products is subject to protection under the copyright laws of the United States.

247. Access to Ubiquiti's Firmware is subject to the Firmware License Agreement and is controlled by technological measures, namely signature protected firmware in the case of

Ubiquiti Firmware versions 5.6.15 and later and software for detecting unauthorized firmware for Ubiquiti Firmware versions 5.6.14 and lower.

248. Cambium, individually and acting in concert and with third parties, has violated Ubiquiti's rights under 17 U.S.C. § 1201(a)(1) by directly circumventing access control measures that effectively control the ability to update or alter the firmware on Ubiquiti M-series devices by using the Hacked Firmware, which passes through Ubiquiti's access control measures for detecting unauthorized firmware, and allows the Hacked Firmware to install on Ubiquiti M-series devices and thereafter make unauthorized access and use of portions of Ubiquiti's copyrighted Firmware to take control of Ubiquiti M-series devices. The Hacked Firmware after installation disables Ubiquiti's access control measures.

249. The conduct described above has cost Ubiquiti an amount to be determined at trial and constitutes a violation of 17 U.S.C. § 1201.

250. The conduct described above was willful and undertaken with knowledge of wrongdoing, and was undertaken with commercial motives to sell licenses to the Hacked Firmware and Cambium hardware to interface with hacked Ubiquiti M-series devices. An award of statutory damages is necessary to dissuade Defendants and others from the use of the Hacked Firmware.

251. Accordingly, pursuant to 17 U.S.C. § 1203, Ubiquiti is entitled to and hereby demands statutory damages in the maximum amount of $2,500 for each of the violations of the statute.

252. Ubiquiti is also entitled to an award of attorneys' fees and costs as provided under 17 U.S.C. § 1203.

253. Cambium's conduct, unless enjoined by the Court, will cause irreparable harm to Ubiquiti, which has no adequate remedy at law. Pursuant to 17 U.S.C. § 1203, Ubiquiti is also entitled to an award of attorneys' fees and costs.

B. DMCA § 1201(a)(2) Violations

254. Section 1201(a)(2) of the DMCA provides that no person shall traffic in any technology, product, service, device, component, or part thereof, that, among other things, is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title.

255. Ubiquiti's Firmware for its M-series products is subject to protection under the copyright laws of the United States.

256. Access to Ubiquiti's Firmware is subject to the Firmware License Agreement and is controlled by technological measures, namely signature protected firmware in the case of Ubiquiti Firmware versions 5.6.15 and later and software for detecting unauthorized firmware for Ubiquiti Firmware versions 5.6.14 and lower.

257. Cambium, individually and collectively, have directly, or acting in concert with a third party, violated Ubiquiti's rights under 17 U.S.C. § 1201(a)(2) by offering to the public, services and the Hacked Firmware to circumvent Ubiquiti's technological measures.

258. Such services include in-person educational seminars demonstrating hacking Ubiquiti M-series devices with Hacked Firmware to circumvent Ubiquiti's technological measures; disseminating quick start guides and on-line videos demonstrating how to circumvent technological measures on Ubiquiti M-series devices and install the Hacked Firmware; and disseminating instructions on how to defeat Ubiquiti's signature protected firmware on Ubiquiti Firmware versions 5.6.15 and later on Cambium's community website

community.cambiumnetworks.com (*See* https://community.cambiumnetworks.com/t5/ePMP-Elevate/Issues-elevating-Ubiquiti-devices-with-firmware-higher-than-5-6/td-p/78837).

259. Cambium traffics in such services and the Hacked Firmware, which are used to disable Ubiquiti's technological measures and make Ubiquiti M-series devices and Ubiquiti Firmware that remains on the Ubiquiti M-series devices available for unauthorized access, copying and use thereafter.

260. The conduct described above has cost Ubiquiti an amount to be determined at trial and constitutes a violation of 17 U.S.C. § 1201.

261. The conduct described above was willful and undertaken with knowledge of wrongdoing, and was undertaken with commercial motives to sell licenses to the Hacked Firmware and Cambium hardware to interface with hacked Ubiquiti M-series devices. An award of statutory damages is necessary to dissuade Defendants and others from the use of the Hacked Firmware.

262. Accordingly, pursuant to 17 U.S.C. § 1203, Ubiquiti is entitled to and hereby demands statutory damages in the maximum amount of $2,500 for each violation of the DMCA.

263. Ubiquiti is also entitled to an award of attorneys' fees and costs as provided under 17 U.S.C. § 1203.

264. Cambium' conduct, unless enjoined by the Court, will cause irreparable harm to Ubiquiti, which has no adequate remedy at law.

C. DMCA § 1202(b) Violations

265. Section 1202(b) of the DMCA provides, among other things, that no person shall, without authorization of the copyright owner or the law intentionally remove or alter any copyright management information, or distribute copyright management information knowing that the copyright management information has been removed or altered without authority, knowing or

having reasonable grounds to know that it will induce, enable, facilitate, or conceal an infringement.

266. Ubiquiti's Firmware for its M-series products is subject to protection under the copyright laws of the United States.

267. Access to Ubiquiti's Firmware is subject to the Firmware License Agreement and is controlled by technological measures, namely signature protected firmware in the case of Ubiquiti Firmware versions 5.6.15 and later and software for detecting unauthorized firmware for Ubiquiti Firmware versions 5.6.14 and lower.

268. Ubiquiti's Firmware also includes user interface software that allows users to interface with Ubiquiti M-series devices and allows users to upload new firmware to Ubiquiti M-series devices. The user interface software within the Ubiquiti Firmware includes copyright management information that is presented to the user on each page of the user interface that identifies Ubiquiti as the copyright owner of the Ubiquiti Firmware for each M-series device.

269. Cambium, individually and collectively, have directly, or acting in concert with a third party, violated Ubiquiti's rights under 17 U.S.C. § 1202(b) by distributing Hacked Firmware directly and through distributors to Ubiquiti customers that circumvents Ubiquiti's technological measures, removes Ubiquiti's user interface software including its copyright management information, and replaces the copyright management information with a new statement that Cambium is the copyright owner.

270. Cambium's conduct has been willful. Despite the fact that Ubiquiti firmware remains on the Ubiquiti M-series device even after it is hacked with the Hacked Firmware by Defendants or a Ubiquiti customer at the urging of Cambium, Cambium has removed the Ubiquiti copyright management information in order to conceal Cambium's infringement of Ubiquiti's

copyrights in the Ubiquiti Firmware, knowing that this will induce and/or facilitate infringement of the Ubiquiti Firmware as the user interacts with the Hacked Firmware on hacked Ubiquiti M-series devices.

271. The conduct described above has cost Ubiquiti an amount to be determined at trial and constitutes a violation of 17 U.S.C. § 1202.

272. The conduct described above was willful and undertaken with knowledge of wrongdoing, and was undertaken with commercial motives to sell licenses to the Hacked Firmware and Cambium hardware to interface with hacked Ubiquiti M-series devices. An award of statutory damages is necessary to dissuade Defendants and others from the use of the Hacked Firmware.

273. Accordingly, pursuant to 17 U.S.C. § 1203, Ubiquiti is entitled to and hereby demands statutory damages in the maximum amount of $2,500 for each of the violations of the statute.

274. Ubiquiti is also entitled to an award of attorneys' fees and costs as provided under 17 U.S.C. § 1203.

275. Cambium's conduct, unless enjoined by the Court, will cause irreparable harm to Ubiquiti, which has no adequate remedy at law.

THIRD CLAIM FOR RELIEF
(Violation of the Illinois Computer Crime Prevention Law, 720 Il. C.S. 5/17-51)
(Asserted Against Cambium)

276. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

277. Ubiquiti's M-series devices are computers which operate using Ubiquiti Firmware licensed by Ubiquiti to M-series device customers.

278. Cambium transmits and aids and abets third parties, including Ubiquiti's customers, in the installation of the Hacked Firmware on Ubiquiti M-series devices in violation of the access restrictions pursuant to Ubiquiti Firmware License Agreements, causing damage to the Ubiquiti M-series devices and the licensed Ubiquiti Firmware, including destroying large portions of the Ubiquiti Firmware, which results in the Ubiquiti M-series devices being impaired, no longer compliant with FCC rules and regulations and no longer able to connect to other Ubiquiti devices using Ubiquiti's wireless protocols.

279. Cambium's conduct is intentional, and without permission of Ubiquiti, and its Hacked Firmware causes the damage to the Ubiquiti M-series devices and Ubiquiti Firmware described above in direct violation of the governing Ubiquiti Firmware Licensing Agreements.

280. Ubiquiti has sustained damage by, *inter alia*, having the Ubiquiti M-series devices and Firmware, which underlie its Firmware License Agreements with customers, impaired and altered and no longer compatible with other Ubiquiti devices using Ubiquiti's wireless protocols.

281. Unless restrained and enjoined, Cambium will continue to commit such acts. Ubiquiti's remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Ubiquiti to remedies, including injunctive relief, or other equitable relief.

FOURTH CLAIM FOR RELIEF
(Willful violation of the Copyright Act, 17 U.S.C. §§ 101, *et seq.*)
(Asserted Against Cambium)

282. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

283. Ubiquiti owns copyrights in the Ubiquiti Firmware and has registered the copyrights. As the owner of the copyrights, Ubiquiti maintains exclusive rights to, *inter alia*,

distribute and reproduce the Ubiquiti Firmware. Ubiquiti licenses the Ubiquiti Firmware on a non-exclusive basis to its customers for use with Ubiquiti M-series devices.

284. Cambium has directly infringed and will continue to infringe Ubiquiti's copyrights in the Ubiquiti Firmware by violating the Ubiquiti Firmware License Agreement and making unauthorized copies and use of Ubiquiti Firmware for Ubiquiti M-series devices.

285. Cambium has directly infringed and will continue to infringe Ubiquiti's copyrights in the Ubiquiti Firmware by hacking into Ubiquiti M-series devices by loading the Hacked Firmware onto M-series devices and causing the Ubiquiti M-series devices to execute the Hacked Firmware. The Hacked Firmware destroys the integrity of the Ubiquiti Firmware, creates an unauthorized derivative work of the Ubiquiti firmware, and makes unauthorized copies of the Ubiquiti firmware, all in violation of the copyright act.

286. Such acts of direct infringement include Cambium's development of the Hacked Firmware, Cambium's demonstration of hacking a Ubiquiti M-series device in instructional videos posted on the Internet, and on information and belief Cambium's demonstration of the infringement by hacking Ubiquiti M-series devices in live classes.

287. Cambium has contributed to and induced the infringement of Ubiquiti's copyrights in the Ubiquiti firmware by third parties, including Cambium's distributors and Ubiquiti customers, by one or more of the following actions: making the Hacked Firmware available for download, marketing and promoting the Hacked Firmware to Ubiquiti's M-series device customers, selling and distributing "licenses" to use the Hacked Firmware on Ubiquiti M-series products, distributing a "Quick Start Guide" instructing Ubiquiti M-series device users how to hack their device with the Hacked Firmware, and providing online videos, customer support and

live demonstrations encouraging and teaching Ubiquiti customers how to hack Ubiquiti M-series devices with Hacked Firmware.

288. The infringing conduct described above has damaged Ubiquiti in an amount to be determined at trial and constitutes violations of 17 U.S.C. § 501. Ubiquiti is entitled to recover, under the Copyright Act, actual damages it has sustained and any gains, profits and advantages obtained by Defendants as a result of their acts of infringement alleged above.

289. The conduct described above was willful, was undertaken with knowledge of wrongdoing, and was undertaken with commercial motives to sell licenses to the Hacked Firmware and Cambium hardware to interface with hacked Ubiquiti M-series devices.

290. Ubiquiti has registered copyrights for the Ubiquiti Firmware that predate the course of Defendants' infringing conduct. Ubiquiti seeks a determination of statutory damages in the maximum amount of $150,000.00 per work infringed in view of the willful and commercially motivated infringement by Cambium pursuant to 17 U.S.C. § 504.

291. Under the Copyright Act, Ubiquiti is entitled to recover costs, including attorneys' fees pursuant to 17 U.S.C. § 505, for Defendants' acts of infringement.

292. Cambium's conduct, unless enjoined by the Court, will cause irreparable harm to Ubiquiti, which has no adequate remedy at law.

293. Cambium's Hacked Firmware, unless impounded and destroyed, will also continue to make unauthorized use of the Ubiquiti firmware in hacked Ubiquiti M-series devices and will cause continuing damage to Ubiquiti.

FIFTH CLAIM FOR RELIEF
(False Advertising under § 43(a) of the Lanham Act, 15 U.S.C. § 1125(a)(1)(B))
(Asserted Against Cambium)

294. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

295. Cambium has disseminated through its promotional materials for the Hacked Firmware, including but not limited to guides and online instructional webinar videos, false and misleading statements concerning Ubiquiti, and the nature and propriety of the Hacked Firmware in violation of § 43(a) of the Lanham Act. Cambium's false and misleading statements include, but are not limited to, statements concerning the amount of firmware from Ubiquiti left on Ubiquiti M-series devices and its use after being hacked with Cambium's Hacked Firmware, statements that a hardware warranty may be available after Hacked Firmware is installed, and statements that FCC compliance on a Ubiquiti M-series device modified with the Hacked Firmware can be ensured by asking the third party manufacturer to apply a new FCC label. These statements constitute false and deceptive advertising and are likely to mislead, and/or have misled, consumers and distributors about the nature, characteristics and quality of the Hacked Firmware. Cambium's false and misleading statements are intended to conceal Cambium's copyright infringement, sell licenses to the Hacked Firmware and Cambium products to interface with hacked Ubiquiti M-series devices, and attack the reputation, goodwill and market position of Ubiquiti.

296. Cambium has willfully, knowingly, and intentionally made and continues to make false descriptions in advertising, and unless enjoined by this Court, will continue to deceive, mislead, and confuse consumers and distributors into believing that, among other things, Cambium's creation and dissemination of Hacked Firmware for Ubiquiti M-series devices is lawful, supported by warranty coverage from Ubiquiti, and yields hacked Ubiquiti M-series

devices that are FCC complaint. Cambium's false and deceptive advertising and promotion of its Hacked Firmware is intentionally and specifically targeted at Ubiquiti M-series devices as part of a deceptive sales strategy to migrate Ubiquiti customers away from Ubiquiti products to Cambium products with which the hacked Ubiquiti M-series devices are compatible.

297. As a direct and proximate cause of Cambium's unlawful acts and practices, including those set forth above, Cambium has caused, is causing, and unless enjoined by this Court, will continue to cause immediate and irreparable harm to Ubiquiti, for which there is no adequate remedy at law, and for which Ubiquiti is entitled to injunctive relief. Cambium's acts, as described herein, are, and unless enjoined, will continue to be, in violation of Section 43(a) of the Lanham Act.

298. As a direct and proximate cause of Cambium's unlawful acts and practices, including those set forth above, Cambium has caused, is causing, and unless enjoined by this Court, will continue to cause Ubiquiti to suffer damages to its business, reputation, and goodwill, and the loss of sales and profits Ubiquiti would have made but for Cambium's acts.

299. Cambium has acted in bad faith and has willfully engaged in false advertising with the intent to injure Ubiquiti and deceive the public. Thus, in addition to the injunctive relief and damages requested herein, Ubiquiti is entitled to costs and attorneys' fees pursuant to 25 U.S.C. § 1117(a).

SIXTH CLAIM FOR RELIEF
(Breach of Contract)
(Asserted Against Cambium)

300. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

301. Cambium has freely entered into Ubiquiti's Firmware License Agreements by using Ubiquiti M-series devices and downloading Ubiquiti firmware and a valid and binding contract has been formed between Cambium and Ubiquiti as set forth in the Ubiquiti Firmware License Agreements.

302. There was valuable consideration exchanged in connection with the Firmware License Agreements. Specifically, Cambium was granted a limited license to use the Ubiquiti Firmware on M-series devices in exchange for Cambium's agreement to comply with the terms of use.

303. The Firmware License Agreements expressly prohibited Cambium from "remov[ing] or alter[ing] any Ubiquiti copyright, trademark or other proprietary rights notices from the Software or Content" including the user interface of the Ubiquiti Firmware or any Ubiquiti Device. *See* Ex. B at 1, 2 and Ex. C at 3.

304. The Firmware License Agreements further provided that Cambium "may not and shall not permit others to," *inter alia*,

> c. copy the Ubiquiti Firmware (except as expressly permitted above), or copy the accompanying documentation;
>
> d. modify, translate, reverse engineer, decompile, disassemble or otherwise attempt (i) to defeat, avoid, bypass, remove, deactivate, or otherwise circumvent any software protection mechanisms in the Ubiquiti Firmware, including without limitation any such mechanism used to restrict or control the functionality of the Ubiquiti Firmware, or (ii) to derive the source code or the underlying ideas, algorithms, structure or organization from the Ubiquiti Firmware (except that the foregoing limitation does not apply to the extent that such activities may not be prohibited under applicable law); or
>
> e. distribute, rent, transfer or grant any rights in the Ubiquiti Firmware or modifications thereof or accompanying documentation in any form to any person without the prior written consent of Ubiquiti.

f. remove any Ubiquiti copyright notice or Ubiquiti branding from the Ubiquiti Firmware or modify any user interface of the Ubiquiti Firmware or Ubiquiti Device.

305. The Firmware License Agreements provided that Cambium not do the following:

> remove or alter any copyright, trademark or other proprietary rights notices from the Software or Content, or use them in contravention of any such applicable notices;
>
> reverse engineer, decompile, translate, disassemble or otherwise attempt to (i) derive the source code or the underlying ideas, algorithms, structure or organization of any Software (except that the foregoing limitation does not apply to the extent that such activities may not be prohibited under applicable law); or (ii) defeat, avoid, bypass, remove, deactivate, or otherwise circumvent any software protection mechanisms in the Software, including, without limitation, any such mechanism used to restrict or control the functionality of the Software;
>
> use the Software in violation of any third-party rights or any local, state, national or international law or regulation, including, without limitation, any local country regulations related to operation within legal frequency channels, output power and Dynamic Frequency Selection (DFS) requirements;

306. Cambium breached the foregoing provisions of the Firmware License Agreements by the conduct described herein.

307. Specifically, Cambium engaged in unauthorized copying and use of the proprietary features of the Ubiquiti Firmware.

308. Cambium's Elevate Firmware Update replaced numerous sections of the Ubiquiti Firmware and used the Ubiquiti Firmware code in the resulting Elevate Firmware Update.

309. Cambium also modified the Ubiquiti Firmware and attempted to defeat, avoid, bypass, remove, deactivate, or otherwise circumvent any software protection mechanisms in the Ubiquiti Firmware, including mechanisms use to control the functioning of the Ubiquiti Firmware.

310. Cambium also reverse engineered the Ubiquiti Firmware in order to create the Cambium Elevate Firmware. The Cambium Elevate Firmware makes unauthorized copies and use of various components of the Ubiquiti Firmware.

311. Cambium's actions resulted in the unauthorized modification of the Ubiquiti Firmware.

312. Cambium's actions of illicit copying and modification of the Ubiquiti Firmware were in violation of, *inter alia*, the copyright laws of the United States.

313. Cambium's breaches of the End User Agreement are material and eviscerate the limited use that Ubiquiti granted.

314. Cambium's breaches have proximately and directly caused damage to Ubiquiti. Users no longer have functioning Ubiquiti Firmware on their devices after installation of the Cambium Hacked Firmware.

SEVENTH CLAIM FOR RELIEF
(Tortious Interference With Contract)
(Asserted Against Cambium)

315. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

316. The Firmware License Agreements are binding and enforceable contracts.

317. Cambium had actual knowledge of the Firmware License Agreements and freely entered into them by virtue of Cambium's use of Ubiquiti M-series devices and firmware as described above.

318. Cambium's false and misleading advertisement and promotion of the Hacked Firmware used to induce end users to install the Hacked Firmware on Ubiquiti M-series devices

constitute intentional acts taken with knowledge that users would be induced into violating the terms of their Firmware License Agreements with Ubiquiti.

319. Cambium configured the Hacked Firmware to make changes to the Ubiquiti Firmware knowing that these changes would breach the express terms of Ubiquiti's Firmware License Agreements with end users.

320. Cambium's interference with the Firmware License Agreements between Ubiquiti and end users has harmed Ubiquiti by having induced and continuing to induce end users to violate the terms of their Firmware License Agreements with Ubiquiti and causing damage to M-series devices rendering them no longer compatible with Ubiquiti protocols used to communicate with other Ubiquiti devices, causing, *inter alia*, lost sales, infringement and reputational harm.

EIGHTH CLAIM FOR RELIEF
(Unfair Competition)
(Asserted Against Cambium)

321. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

322. Ubiquiti has invested considerable money and time into developing the Ubiquiti Firmware.

323. Cambium has reverse engineered the Ubiquiti Firmware to reap the benefits of Ubiquiti's substantial investment of time and money and to free-ride on Ubiquiti's costly investment.

324. Cambium also unfairly benefits from Ubiquiti's investment into development of the Ubiquiti Firmware insofar as the Cambium Elevate Firmware makes use of and alters elements from the Ubiquiti Firmware.

325. Cambium, through its videos targeting Ubiquiti customers and posting on message boards targeting Ubiquiti customers, has propagated false and misleading promotional materials for the Hacked Firmware and maliciously interfered with Ubiquiti's customer relationships in an effort to mislead and induce those customers become customers of Cambium.

326. Cambium's reverse engineering and use of Ubiquiti's firmware in connection with the launch of the Cambium's Hacked Firmware for Ubiquiti M-series devices also constitutes unfair competition.

327. Cambium's Hacked Firmware is a competing product to Ubiquiti's firmware for M-series devices that is promoted with misleading statements and that after installation damages Ubiquiti firmware on M-series devices.

328. Cambium and Ubiquiti are competitors in wireless devices and in the dissemination of firmware for wireless devices.

329. Cambium's alteration of the Ubiquiti firmware damages and otherwise dilutes the quality of the Ubiquiti Firmware and harms Ubiquiti and its customers who purchased the Ubiquiti product.

330. Cambium's unfairly competitive behavior has proximately and directly caused damage to Ubiquiti.

NINTH CLAIM FOR RELIEF
(Intentional Interference with Prospective Economic Advantage)
(Asserted Against Cambium)

331. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

332. Ubiquiti had a reasonable opportunity to obtain business advantage from customers and prospective customers who would purchase and make use of the Ubiquiti firmware.

333. Cambium was aware of Ubiquiti's relationship with current customers and expectations of obtaining business from its existing and other customers.

334. Indeed, Cambium specifically advertised the Hacked Firmware using deceptive and misleading descriptions to Ubiquiti customers and prospective customers.

335. Cambium intentionally and unjustifiably interfered with Ubiquiti's relationships with current and prospective customers.

336. Cambium unjustifiably misled and induced customers of Ubiquiti to install the Hacked Firmware in violation of Ubiquiti Firmware License Agreements, altering the Ubiquiti firmware on Ubiquiti M-series devices so that customers of Ubiquiti could no longer use the hacked M-series devices to communicate with other Ubiquiti devices using Ubiquiti wireless protocols, but instead could communicate with Cambium products.

337. Cambium induced customers to terminate and not enter into certain business relationships with Ubiquiti for the sale of Ubiquiti devices to communicate with the installed base of hacked Ubiquiti M-series running the Hacked Firmware.

338. Ubiquiti has thus lost both current and prospective customers and sales as a result of Cambium's deceptive and misleading actions and has been damaged as a result.

TENTH CLAIM FOR RELIEF
(Infringement of Registered Trademarks, § 32 Lanham Act, 15 U.S.C. § 1114)
(Asserted Against Cambium)

339. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

340. Cambium, without authorization from Ubiquiti, is using in interstate commerce for the purpose of promoting the downloading and use of Cambium's Hacked Firmware on Ubiquiti's M-series devices, the following Ubiquiti registered trademarks: UBIQUITI®, NANOSTATION®,

NANOBEAM®, NANOBRIDGE®, ROCKET®, and POWERBEAM®, in violation of § 32 of the Lanham Act.

341. Cambium's conduct is likely to have caused and will continue to cause confusion, mistake and deception among consumers as to the source, origin, sponsorship or approval by Ubiquiti of Cambium's Hacked Firmware for Ubiquiti's M-series devices.

342. Cambium's conduct is willful and an intentional violation of Ubiquiti's rights under § 32 of the Lanham Act, 15 U.S.C. § 1114.

ELEVENTH CLAIM FOR RELIEF
(False Designation of Origin, § 43(a) Lanham Act, 15 U.S.C. § 1125(a)(1)(A))
(Asserted Against Cambium)

343. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

344. Cambium, without authorization from Ubiquiti, is using Ubiquiti trademarks, including UBIQUITI®, NANOSTATION®, NANOBEAM®, NANOBRIDGE®, ROCKET®, and POWERBEAM®, for the purpose of promoting the downloading and use of its Hacked Firmware on Ubiquiti's M-series devices, in violation of § 43(a) of the Lanham Act.

345. Cambium's conduct is likely to have caused and will continue to cause confusion, mistake and deception among consumers as to the source, origin, sponsorship or approval by Ubiquiti of Cambium's Hacked Firmware for Ubiquiti's M-series devices.

346. Cambium's conduct is willful and an intentional violation of Ubiquiti's rights under § 43(a) of the Lanham Act, 15 U.S.C. § 1125(a)(1)(A).

TWELFTH CLAIM FOR RELIEF
(Common Law Trademark Infringement)
(Asserted Against Cambium)

347. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

348. Cambium, without authorization from Ubiquiti, is using Ubiquiti trademarks, including UBIQUITI, NANOSTATION, NANOBEAM, NANOBRIDGE, ROCKET, and POWERBEAM, for the purpose of promoting the downloading and use of its Hacked Firmware on Ubiquiti's M-series devices, in violation of § 43(a) of the Lanham Act.

349. Cambium's conduct is likely to have cause and will continue to cause confusion, mistake and deception among consumers as to the source, origin, sponsorship or approval by Ubiquiti of Cambium's Hacked Firmware for Ubiquiti's M-series devices.

350. Cambium's conduct is willful and an intentional violation of Ubiquiti's common law trademark rights.

THIRTEENTH CLAIM FOR RELIEF
(Common Law Misappropriation)
(Asserted Against Cambium)

351. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

352. Ubiquiti invested considerable time and money into developing its Ubiquiti firmware, Ubiquiti M-series devices, and its brand recognition.

353. Cambium misappropriated the Ubiquiti firmware, by distributing Hacked Firmware that still uses Ubiquiti firmware, deceiving customers regarding the nature of the Hacked Firmware, and inducing such customers to alter the Ubiquiti firmware on Ubiquiti M-series

devices with the Hacked Firmware in violation of the Ubiquiti Firmware License Agreements at little or no cost to Cambium.

354. Cambium has also improperly traded and attempted to induce business for itself by misusing the Ubiquiti name deceiving customers regarding the nature of the Hacked Firmware to induce customers to hack Ubiquiti M-series devices and purchase and install Cambium products.

355. As a direct and proximate result of Cambium's misappropriation of Ubiquiti's firmware, Ubiquiti M-series devices, and its brand recognition, Cambium has obtained new customers and a free ride from the use of Ubiquiti's firmware because Cambium bore little or no expense in acquiring customers and inducing those customers to alter and continue to use portions of the Ubiquiti firmware.

356. As a direct and proximate result of Cambium's misappropriation of Ubiquiti's firmware, Ubiquiti M-series devices, and its brand recognition, Ubiquiti has suffered damages, including reputational harm, loss of business, and commercial damage in the marketplace.

FOURTEENTH CLAIM FOR RELIEF
(Violation of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962(c))
(Asserted Against Cambium)

357. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

358. Cambium, Cambium Networks, Winncom, Dmitry Moiseev, and Sakid Ahmed comprise the Hacking Enterprise. The Hacking Enterprise is an association-in-fact enterprise engaged in activities that affect interstate commerce.

359. Cambium oversees the Hacking Enterprise running its day-to-day operations, with Winncom serving Cambium's needs within the Hacking Enterprise.

360. Winncom reports to Cambium regarding its distribution and sales.

361. Cambium, in turn, keeps Cambium Networks apprised of the Hacking Enterprises' activities, profits, and distributions thereof.

362. Cambium agreed to and did conduct and participate in the conduct of the Hacking Enterprise's affairs through a pattern of racketeering activity and for the unlawful purpose of intentionally defrauding consumers into installing the Hacked Firmware, which in turn ensured financial gains for the Hacking Enterprise members above and beyond those which the members would have received had then been engaging solely in lawful activities.

363. To the extent known at this time and to be further developed through discovery of information exclusively within the possession, custody, control and knowledge of the Hacking Enterprise members, that pattern includes related acts of mail fraud and wire fraud, including, but not limited to the activities described in paragraphs 93-105, 110-126, 160, *supra*.

364. Cambium was involved in each of these racketeering acts, specifically orchestrating and arranging for the racketeering acts to occur through the Hacking Enterprise.

365. The acts set forth above, which happened over a period of years, constitute a pattern of racketeering activity pursuant to 18 U.S.C. § 1961(5).

366. Because the Hacking Enterprise directly targeted Ubiquiti customers, Ubiquiti has lost customers as a result of the Hacking Enterprises' activities.

367. Given false and misleading statements and material omissions made by the members of the Hacking Enterprise through the wires and mail, Ubiquiti has lost consumer good will in the market place and its brand reputation has been harmed.

368. As a direct and proximate result of Cambium's racketeering activities and violations of 18 U.S.C. § 1962(c), Ubiquiti has been injured in its business and property in that:

Ubiquiti has lost customers and customers were induced to breach the terms of the Ubiquiti's Firmware Licensing Agreements, Ubiquiti's M-series devices and licensed firmware have been damaged by eliminating their compatibility with other Ubiquiti networking devices using Ubiquiti protocols, and Ubiquiti's licensed intellectual property rights have been violated, in each case through installation of the Hacked Firmware.

369. Thus, Ubiquiti prays that the Court compensate Ubiquiti for Cambium's racketeering activities and grant Ubiquiti legal relief to remedy Cambium's RICO violations.

370. As a result of Cambium's RICO violations, Ubiquiti has lost sales and prospective sales to consumers, in an amount to be determined at trial. Specifically, customers of Ubiquiti have—at the direction and bequest of Cambium and after hearing Cambium's false and inaccurate statements—installed the Hacked Firmware altering their Ubiquiti devices rendering them unable able to communicate with other Ubiquiti products using Ubiquiti protocols.

371. Cambium should be ordered to pay to Ubiquiti damages for Cambium's RICO violations which have resulted in the concrete financial losses outlined herein.

372. Ubiquiti is entitled to treble damages for the RICO violations alleged herein

FIFTEENTH CLAIM FOR RELIEF
(Violation of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962(d))
(Asserted Against Cambium Networks, Blip, Winncom, Sakid Ahmed, and Dmitry Moiseev)

373. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

374. In commission of the racketeering acts set forth herein, each member of the Hacking Enterprise and co-conspirator Blip conspired to violate the RICO statute in violation of 18 U.S.C. § 1962(d).

375. Specifically, the Hacking Enterprise members and co-conspirator Blip worked together to ensure financial gain at the expense of Ubiquiti's copyrights, trademarks, and customer base.

376. The members of the Hacking Enterprise worked together to exceed the permissible and ordinary scope of a manufacturer-distributor relationship. So too did co-conspirator Blip work with Cambium to exceed the ordinary scope of a manufacturer-distributor relationship.

377. The members of the Hacking Enterprise conspired together to promote false advertisement to customers through webinars and in person demonstrations involved the Hacked Firmware.

378. Each of the members of the Hacking Enterprise as well as co-conspirator Blip were aware of the fraudulent nature and scope of the Hacking Enterprise and agreed to assist the Hacking Enterprise in carrying out its fraudulent acts.

379. Each of the members of the Hacking Enterprise agreed to the commission of, or participate in, at least two of the racketeering acts described herein. So too did Blip.

380. Indeed, each of the members of the Hacking Enterprise was aware of the Hacking Enterprise and received direct personal financial gain from the activities of the Hacking Enterprise. Likewise, Blip received direct financial benefit as a result of the Hacking Enterprise's activities.

381. Each of the members of the Hacking Enterprise and co-conspirator Blip intended to and in fact did further the purposes of the Hacking Enterprise.

382. Each of the members of the Hacking Enterprise and co-conspirator Blip engaged in the RICO conspiracy in order to further their own personal interests and ensure financial health for themselves individually.

383. Each of the members of the Hacking Enterprise and co-conspirator Blip wanted to harm Ubiquiti's goodwill and customer standing in the market place.

384. Each of the members of the Hacking Enterprise was aware of Cambium's control and worked together to further that control. Blip likewise aided Cambium in its control of the Hacking Enterprise and profit seeking motive.

385. Cambium took the control of the Enterprise.

386. Cambium Networks placed Cambium at the helm and allowed Cambium to run the U.S. sales and operations of the Hacked Firmware.

387. Dmitry Moiseev and Sakid Ahmed advertised the Hacked firmware, monitored web boards pertaining to the Hacked Firmware, and answered individual questions from users regarding the Hacked Firmware.

388. Blip and Winncom conspired with Cambium to ensure Cambium's position of control in the Hacking Enterprise and supported Cambium's efforts to market the Hacked Firmware.

389. Cambium Networks provided financial support to Cambium to ensure its position as the leader of the Hacking Enterprise and also authorized discounts and personal financial gains for Blip and Winncom.

390. The members of the Hacking Enterprise knew that their actions were part of a pattern of racketeering activity and agreed to commit their actions in furtherance of the scheme described herein. This conduct constitutes a conspiracy to violate 18 U.S.C. § 1962(c), in violation of 18 U.S.C. § 1962(d).

391. Blip likewise worked with Cambium to ensure Cambium's role as the lead of the Hacking Enterprise, and knew that Cambium was carrying out a pattern of racketeering activity

along with various other members of the Hacking Enterprise and agreed to have Cambium commit its racketeering activities along with co-conspirators in furtherance of the scheme described herein. This conduct constitutes a conspiracy to violate 18 U.S.C. § 1962(c), in violation of 18 U.S.C. § 1962(d).

392. Each of the members of the Hacking Enterprise and co-conspirator Blip were aware that Cambium was directly targeting Ubiquiti customers and making misleading claims implying that the Hacked Firmware was appropriately used with Ubiquiti products.

393. The Hacking Enterprise is an enterprise engaged in and whose activities affect interstate commerce.

394. As a direct and proximate result of the Hacking Enterprise's conspiracy, conspiracy with Blip, and RICO violations flowing therefrom, Ubiquiti has been injured in its business and property in that Ubiquiti has lost customers, had its copyrights and trademarks violated by the Hacking Enterprise, and had its M-series devices converted to ones that are no longer FCC complaint and not compatible with Ubiquiti protocols used to communicate with other products sold by Ubiquiti.

395. Thus, Ubiquiti prays that the Court remedy the co-conspirators racketeering activities and grant Ubiquiti legal relief.

396. As a result of the co-conspirators' RICO violations, Ubiquiti has lost sales and prospective sales to consumers, in an amount to be determined at trial. Specifically, customers of Ubiquiti have—at the direction and bequest of Cambium and after hearing Cambium's false and inaccurate statements—installed the Hacked Firmware converting their Ubiquiti devices to ones no longer compliant with FCC rules and not compatible with Ubiquiti protocols used to communicate with other products sold by Ubiquiti.

397. Ubiquiti is entitled to damages for the Hacking Enterprise's RICO violations, carried out with the knowing assistance of co-conspirator Blip, which have resulted in the concrete financial losses outlined herein in the form of lost profits and customers.

398. Ubiquiti is entitled to treble damages for the RICO violations alleged herein.

RELIEF REQUESTED

WHEREFORE, Ubiquiti Networks, Inc. requests judgment against Defendants and seeks relief, as follows:

A. That judgment be entered for Ubiquiti and against Defendants on all Counts;

B. That this Court find that Cambium violated the Computer Fraud and Abuse Act;

C. That this Court find that Cambium has willfully engaged in false advertising in the promotion of its Hacked Firmware for Ubiquiti M-series devices;

D. That this Court find that Cambium breached its contract with Ubiquiti by violating the Ubiquiti Firmware License Agreements associated with the Ubiquiti Firmware and Ubiquiti M-series devices;

E. That Cambium, its officers, directors, agents, employees, affiliates, subsidiaries, and all other persons acting in concert with them, be temporarily, preliminarily, and permanently enjoined from directly or indirectly creating, distributing or promoting Hacked Firmware.

F. That Cambium be required to account for all gains, profits, and advantages derived from their acts of hacking, false advertising, and infringement and for their other violations of law;

G. That Ubiquiti be awarded its actual damages and any profits attributable to Defendants' causing damage and loss to Ubiquiti by virtue of its hacking and distribution of Hacked Firmware targeting Ubiquiti M-series devices to Ubiquiti's customers, false advertising directed to Ubiquiti's customers, tortious interference and unfair competition directed towards

Ubiquiti's customers and other trademark infringement, copyright infringement and violations of state and federal law.

H. That Defendants be required to deliver for impounding during the pendency of this action, and for destruction, all copies, reproductions, or derivative works of Ubiquiti Firmware or Hacked Firmware in Cambium's possession, custody or control and other promotional material targeting Hacked Firmware for Ubiquiti products;

I. That Defendants be required to retrieve and destroy all copies of the Hacked Firmware provided to distributors, customers and other agents and cancel all "licenses" to the Hacked Firmware.

J. That Defendants be required to delete permanently from Defendants' computers and information technology systems all electronic copies of Ubiquiti Firmware and the Hacked Firmware;

K. That Defendants be required to delete permanently, from any website that they own or control, all copies or reproductions of the Hacked Firmware and related promotional materials;

L. The Court award actual, exemplary and treble damages for the RICO violations.

M. That Ubiquiti be awarded reasonable attorneys' fees and costs incurred in connection with this action, including, but not limited to, reasonable attorneys' fees and costs incurred in connection with Defendants' violation of the Computer Fraud and Abuse Act, the Illinois Computer Crime Prevention Law, the Lanham Act, the Copyright Act, and the RICO Act.

N. That a jury hear Ubiquiti's claims; and,

O. That this Court grant any such other and further relief as it deems just and proper.

Dated: August 7, 2018

Respectfully submitted,

MORGAN, LEWIS & BOCKIUS LLP

/s/ *Elizabeth B. Herrington*

Elizabeth B. Herrington (IL Bar No. 6244547)
77 West Wacker Drive
Chicago, IL 60601-5094
312.324.1000 (Telephone)
312.324.1001 (Facsimile)
beth.herrington@morganlewis.com

Robert C. Bertin
1111 Pennsylvania Avenue, NW
Washington, DC 20004-2541
202.739.3000 (Telephone)
202.739.3001 (Facsimile)
robert.bertin@morganlewis.com

Mark L. Krotoski
1400 Page Mill Road
Palo Alto, CA 94304-1124
650.843.4000 (Telephone)
650.843.4001 (Facsimile)
mark.krotoski@morganlewis.com

Amy M. Dudash
1701 Market Street
Philadelphia, PA 19103
215.963.5000 (Telephone)
215.963.5001 (Facsimile)
amy.dudash@morganlewis.com

Attorneys for Plaintiff Ubiquiti Networks, Inc.

Exhibit A

Certificate of Registration

This Certificate issued under the seal of the Copyright Office in accordance with title 17, *United States Code*, attests that registration has been made for the work identified below. The information on this certificate has been made a part of the Copyright Office records.

Acting United States Register of Copyrights and Director

Registration Number
TXu 1-795-146

Effective date of registration:
April 3, 2012

Title

Title of Work: AirOS 5.2.1

Completion/Publication

Year of Completion: 2010

Author

- **Author:** Ubiquiti Networks, Inc.

Author Created: computer program

Work made for hire: Yes

Citizen of: United States **Domiciled in:** United States

Copyright claimant

Copyright Claimant: Ubiquiti Networks, Inc.
91 E. Tasman Drive, San Jose, CA, 95035, United States

Limitation of copyright claim

Material excluded from this claim: computer program, Previous versions and licensed-in materials

New material included in claim: new and revised computer code

Certification

Name: Jessica Zhou, Ubiquiti Networks, Inc.

Date: April 3, 2012

Applicant's Tracking Number: 70730-50001.00

Registration #: TXU001795146

Service Request #: 1-747770041

Morrison & Foerster LLP
Jennifer Lee Taylor
425 Market Street
San Francisco, CA 94105-2482 United States

Certificate of Registration

This Certificate issued under the seal of the Copyright Office in accordance with title 17, *United States Code*, attests that registration has been made for the work identified below. The information on this certificate has been made a part of the Copyright Office records.

Acting United States Register of Copyrights and Director

Registration Number
TXu 1-795-147

Effective date of registration:
April 3, 2012

Title

Title of Work: AirOS 5.3

Completion/Publication

Year of Completion: 2011

Author

- **Author:** Ubiquiti Networks, Inc.

Author Created: computer program

Work made for hire: Yes

Citizen of: United States **Domiciled in:** United States

Copyright claimant

Copyright Claimant: Ubiquiti Networks, Inc.
91 E. Tasman Drive, San Jose, CA, 95035, United States

Limitation of copyright claim

Material excluded from this claim: computer program, Previous versions and licensed-in materials

New material included in claim: computer program, New and revised computer code

Certification

Name: Jessica Zhou, Ubiquiti Networks, Inc.

Date: April 3, 2012

Applicant's Tracking Number: 70730-50001.00

Registration #: TXU001795147

Service Request #: 1-747770159

Morrison & Foerster LLP
Jennifer Lee Taylor
425 Market Street
San Francisco, CA 94105-2482 United States

Exhibit B

This License Agreement strictly prohibits You from using the Ubiquiti Firmware on any device other than a Ubiquiti Device. You are also prohibited from removing or modifying any Ubiquiti copyright notice, trademark or user interface of the Ubiquiti Firmware or any Ubiquiti Device.

The Ubiquiti Firmware is copyright-protected material under United States and international copyright and other applicable laws. Unauthorized copying, use or modification of ANY PART of this firmware, or violation of the terms of this Agreement, will be prosecuted under the law.

NOTICE

This is an agreement between You and Ubiquiti Networks, Inc. ("Ubiquiti"). YOU MUST READ AND AGREE TO THE TERMS OF THIS FIRMWARE LICENSE AGREEMENT ("AGREEMENT") BEFORE ANY UBIQUITI FIRMWARE CAN BE DOWNLOADED OR INSTALLED OR USED. BY CLICKING ON THE "ACCEPT" BUTTON OF THIS AGREEMENT, OR DOWNLOADING UBIQUITI FIRMWARE, OR INSTALLING UBIQUITI FIRMWARE, OR USING UBIQUITI FIRMWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE WITH THE TERMS AND CONDITIONS OF THIS AGREEMENT, THEN YOU SHOULD EXIT THIS PAGE AND NOT DOWNLOAD OR INSTALL OR USE ANY UBIQUITI FIRMWARE. BY DOING SO YOU FOREGO ANY IMPLIED OR STATED RIGHTS TO DOWNLOAD OR INSTALL OR USE UBIQUITI FIRMWARE.

DEFINITIONS

For the purpose of this Agreement, the following terms shall have the following meanings:

- - "Open Source Software" means any software or software component, module or package that contains, or is derived in any manner (in whole or in part) from, any software that is distributed as free software, open source software or similar licensing or distribution models, including, without limitation, software licensed or distributed under any of the following licenses or distribution models, or licenses or distribution models similar to any of the following: (a) GNU's General Public License (GPL) or Lesser/Library GPL (LGPL); (b) the Artistic License (e.g., PERL); (c) the Mozilla Public License; (d) the BSD License; and (e) the Apache License;
- - "Ubiquiti Device" means a Ubiquiti networking device that You purchase or otherwise rightfully acquire;
- - "Ubiquiti Firmware" means the firmware in object code form made available by Ubiquiti for Ubiquiti Devices; and
- - "You(r)" means the company, entity or individual who owns or otherwise rightfully acquires the Ubiquiti Device into which the Ubiquiti Firmware will be incorporated.

LICENSE GRANT

Ubiquiti grants You a non-exclusive, non-transferable license to use the copy of the Ubiquiti Firmware and accompanying documentation and any updates or upgrades thereto provided by Ubiquiti according to the terms set forth below.

USES AND RESTRICTIONS

You may:

a. download and use the Ubiquiti Firmware solely in Ubiquiti Devices, and make copies of the Ubiquiti Firmware as reasonably necessary for such use, provided that You reproduce, unaltered, all proprietary notices on or in the copies.

You may not, and shall not permit others to:

a. use the Ubiquiti Firmware on any devices or products that are not owned by You or Your business organization;
b. use the Ubiquiti Firmware on any non-Ubiquiti Devices;
c. copy the Ubiquiti Firmware (except as expressly permitted above), or copy the accompanying documentation;
d. modify, translate, reverse engineer, decompile, disassemble or otherwise attempt (i) to defeat, avoid, bypass, remove, deactivate, or otherwise circumvent any software protection mechanisms in the Ubiquiti Firmware, including without limitation any such mechanism used to restrict or control the functionality of the Ubiquiti Firmware, or (ii) to derive the source code or the underlying ideas, algorithms, structure or organization from the Ubiquiti Firmware (except that the foregoing limitation does not apply to the extent that such activities may not be prohibited under applicable law); or
e. distribute, rent, transfer or grant any rights in the Ubiquiti Firmware or modifications thereof or accompanying documentation in any form to any person without the prior written consent of Ubiquiti.
f. remove any Ubiquiti copyright notice or Ubiquiti branding from the Ubiquiti Firmware or modify any user interface of the Ubiquiti Firmware or Ubiquiti Device.

The Ubiquiti devices must be properly installed. It is your responsibility to follow local country regulation including operation within legal frequency channels, output power, and Dynamic Frequency Selection (DFS) requirements. You are responsible for keeping the devices working according to these rules.

This license is not a sale. Title and copyrights to the Ubiquiti Firmware, and any copy made by You remain with Ubiquiti and its suppliers. Unauthorized copying of the Ubiquiti Firmware or the accompanying documentation, or failure to comply with the above restrictions, will result in automatic termination of this license and will make available to Ubiquiti other legal remedies.

OPEN SOURCE SOFTWARE

You hereby acknowledge that the Ubiquiti Firmware may contain Open Source Software. You agree to review any documentation that accompanies the Ubiquiti Firmware or is identified

in the documentation for the Ubiquiti Firmware in order to determine which portions of the Ubiquiti Firmware are Open Source Software and are licensed under an Open Source Software license. To the extent any such license requires that Ubiquiti provide You the rights to copy, modify, distribute or otherwise use any Open Source Software that are inconsistent with the limited rights granted to You in this Agreement, then such rights in the applicable Open Source Software license shall take precedence over the rights and restrictions granted in this Agreement, but solely with respect to such Open Source Software. You acknowledge that the Open Source Software license is solely between You and the applicable licensor of the Open Source Software. You shall comply with the terms of all applicable Open Source Software licenses, if any. Copyrights to the Open Source Software are held by the copyright holders indicated in the copyright notices in the corresponding source files or as disclosed at http://www.ubnt.com.

TERMINATION

This license will continue until terminated. Unauthorized copying of the Ubiquiti Firmware or failure to comply with the above restrictions will result in automatic termination of this Agreement and will make available to Ubiquiti other legal remedies. This license will also automatically terminate if You go into liquidation, suffer or make any winding up petition, make an arrangement with Your creditors, or suffer or file any similar action in any jurisdiction in consequence of debt. Upon termination of this license for any reason You will destroy all copies of the Ubiquiti Firmware. Any use of the Ubiquiti Firmware after termination is unlawful.

CONSENT TO USE OF DATA

You agree that Ubiquiti may from time to time collect and use device information (such as hardware model, firmware version, device identifiers, device performance information and device operation parameters), collected in a form that does not personally identify you, to facilitate the provision of Ubiquiti Firmware updates, authenticate Ubiquiti products, verify compliance with the terms of this Agreement, and improve Ubiquiti's products and services.

WARRANTY DISCLAIMER

THE UBIQUITI FIRMWARE, INCLUDING WITHOUT LIMITATION ANY OPEN SOURCE SOFTWARE, AND ANY ACCOMPANYING DOCUMENTATION ARE PROVIDED "AS IS" AND UBIQUITI AND ITS SUPPLIERS MAKE, AND YOU RECEIVE, NO WARRANTIES OR CONDITIONS, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE OR IN ANY COMMUNICATION WITH YOU, AND UBIQUITI AND ITS SUPPLIERS SPECIFICALLY DISCLAIM ANY IMPLIED WARRANTY OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT AND THEIR EQUIVALENTS. Ubiquiti does not warrant that the operation of the Ubiquiti Firmware will be uninterrupted or error free or that the Ubiquiti Firmware will meet Your specific requirements. You acknowledge that Ubiquiti has no support or maintenance obligations for the Ubiquiti Firmware.

LIMITATION OF LIABILITY

EXCEPT TO THE EXTENT THAT LIABILITY MAY NOT BY LAW BE LIMITED OR EXCLUDED, IN NO EVENT WILL UBIQUITI OR ITS SUPPLIERS BE LIABLE FOR LOSS OF OR CORRUPTION TO DATA, LOST PROFITS OR LOSS OF CONTRACTS, COST OF PROCUREMENT OF SUBSTITUTE PRODUCTS OR OTHER SPECIAL, INCIDENTAL, PUNITIVE, CONSEQUENTIAL OR INDIRECT DAMAGES ARISING FROM THE SUPPLY OR USE OF THE UBIQUITI FIRMWARE, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY (INCLUDING WITHOUT LIMITATION NEGLIGENCE). THIS LIMITATION WILL APPLY EVEN IF UBIQUITI OR AN AUTHORIZED DISTRIBUTOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY. IN NO EVENT SHALL UBIQUITI'S OR ITS SUPPLIERS' LIABILITY EXCEED FIVE HUNDRED DOLLARS (US $500). YOU ACKNOWLEDGE THAT THIS PROVSION REFLECTS A REASONABLE ALLOCATION OF RISK.

GENERAL

This Agreement shall not be governed by the 1980 U.N. Convention on Contracts for the International Sale of Goods; rather, this Agreement shall be governed by the laws of the State of California, including its Uniform Commercial Code, without reference to conflicts of laws principles. This Agreement is the entire agreement between us and supersedes any other communications or advertising with respect to the Ubiquiti Firmware and accompanying documentation. If any provision of this Agreement is held invalid or unenforceable, such provision shall be revised to the extent necessary to cure the invalidity or unenforceability, and the remainder of the Agreement shall continue in full force and effect. If You are acquiring the Ubiquiti Firmware on behalf of any part of the U.S. Government, the following provisions apply. The Ubiquiti Firmware and accompanying documentation are deemed to be "commercial computer software" and "commercial computer software documentation", respectively, pursuant to DFAR Section 227.7202 and FAR 12.212(b), as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Ubiquiti Firmware and/or the accompanying documentation by the U.S. Government or any of its agencies shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement. Any technical data provided that is not covered by the above provisions is deemed to be "technical data-commercial items" pursuant to DFAR Section 227.7015(a). Any use, modification, reproduction, release, performance, display or disclosure of such technical data shall be governed by the terms of DFAR Section 227.7015(b).

Ubiquiti Networks is a trademark of Ubiquiti Networks, Inc. in the United States and worldwide.

Exhibit C

End User License Agreement

Legal Documentation

Terms of Service
EULA
Privacy Policy
Limited Warranty
UniFi Elite Terms and Conditions
UBNT Store Terms and Conditions
UniFi IOS App License
Compliance Information

OUR EULA WAS UPDATED ON JULY 17, 2017

This End User License Agreement (this "**EULA**") governs Your access and use of the software ("**Software**") that is embedded on any Ubiquiti Networks, Inc. product ("**Product**").

The term "**You**," "**Your**," "**you**" or "**your**" as used in this EULA, means any person or entity who accesses or uses the Software and accepts the terms of this EULA, including any individuals that You authorize to use or access the Software, including Your independent contractors or employees ("**Authorized Users**"). For the avoidance of doubt, where the term "You," "Your," "you" or "your" is used in this EULA, it shall include any Authorized User, regardless of whether "Authorized User" is specifically stated.

FOR IMPORTANT DISCLAIMERS OF WARRANTY AND WARNINGS CONCERNING USAGE, SEE SECTION V.

YOU MUST READ AND AGREE TO THE TERMS OF THIS EULA BEFORE USING, DOWNLOADING OR INSTALLING ANY SOFTWARE. BY USING, DOWNLOADING OR INSTALLING THE SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS EULA. IF YOU DO NOT AGREE WITH THE TERMS AND CONDITIONS OF THIS EULA, YOU MAY NOT USE, DOWNLOAD OR INSTALL THE SOFTWARE.

THE SOFTWARE MAY BE SUBJECT TO AUTOMATIC SOFTWARE UPDATES, AS DESCRIBED FURTHER IN SECTION III, AND YOU ALSO HEREBY CONSENT TO SUCH UPDATES. If You do not

agree to such updates, You are not permitted to, and You must not, download, install, access or use the Software.

Ubiquiti may, in its sole and absolute discretion, change the terms of this EULA from time to time, as indicated by the date at the end of this EULA. If You object to any such change, Your sole recourse will be to cease using the Software. Continued use of the Software following any such change will indicate Your acknowledgement of such change and agreement to be bound by the new terms and conditions.

I. Overview, Eligibility

a. This EULA is a binding agreement between You and Ubiquiti Networks, Inc. ("**Ubiquiti**").

b. Your use of (1) websites located at www.ubnt.com and ubnt.com sub-domains and any other websites hosted by Ubiquiti or its affiliates, (2) services accessible or downloadable through the Sites, (3) software that may be downloaded to Your smartphone or tablet to access services and (4) subscription services, including services that can be accessed using the Web Apps and Mobile Apps is governed by the Terms of Service. Your purchase of the Product (excluding the Software) is governed by the Limited Warranty. All additional guidelines, terms, or rules on the Sites, including the Privacy Policy, are incorporated by reference into this EULA and You are agreeing to accept and abide by them by using the Software.

c. Subject to Section (I)(d), You may access and use the Software only if You can form a binding contract with Ubiquiti and only if You are in compliance with the terms of this EULA and all applicable laws and regulations. If You are accepting the terms of this EULA on behalf of an entity or individual, You represent and warrant that You have full legal authority to bind such entity or individual to this EULA. You are fully responsible for any Authorized User's compliance with this EULA.

d. If You are an Authorized User, You represent and warrant that You are over the age of 13 (or equivalent minimum age in the jurisdiction where You reside or access or use the Software), and in the event You are between the age of 13 (or equivalent minimum age in the jurisdiction where you reside or access or use the Software) and the age of majority in the jurisdiction where You reside or access or use the Software, that You will only use the Software under the supervision of a parent or legal guardian who agrees to be bound by this EULA. Any use or access to the Software by individuals under the age of 13 (or equivalent minimum age in the jurisdiction where you reside or access or use the Services) is strictly prohibited and a violation of this EULA.

II. License.

a. **License Grant**. Subject to Your compliance at all times with the terms and restrictions set forth in this EULA, Ubiquiti grants You, under its rights in and to the Software, a worldwide, non-sublicensable, non-transferable, non-exclusive, revocable, limited license to download and use the Software in object code form only, solely in connection with the Product that You own or control.

b. **Limitations on Use**.

i. The Software, its contents, features and functionality (including, without limitation, all user interfaces, information, software, code, text, graphics, images, video and audio, and the design, selection and arrangement thereof) (collectively, the "**Content**") are protected by United States and international copyright, trademark, patent, trade secret and other intellectual property or proprietary rights laws.

ii. You shall not directly or indirectly do any of the following:

1. use the Software on any device other than a Product that is owned or controlled by You or Your business organization;
2. sell, offer for sale, lease, license, sublicense or distribute the Software or any Content in any form without the prior written consent of Ubiquiti;
3. copy, reproduce, broadcast, transmit, republish, distribute, modify, prepare derivative works of, perform, publicly perform or display the Software or any Content in any way without the prior written consent of Ubiquiti and its applicable licensors;
4. remove or alter any copyright, trademark or other proprietary rights notices from the Software or Content, or use them in contravention of any such applicable notices;
5. reverse engineer, decompile, translate, disassemble or otherwise attempt to (i) derive the source code or the underlying ideas, algorithms, structure or organization of any Software (except that the foregoing limitation does not apply to the extent that such activities may not be prohibited under applicable law); or (ii) defeat, avoid, bypass, remove, deactivate, or otherwise circumvent any software protection mechanisms in the Software, including, without limitation, any such mechanism used to restrict or control the functionality of the Software;
6. use the Software in violation of any third-party rights or any local, state, national or international law or regulation, including, without limitation, any local country regulations related to operation within legal frequency channels, output power and Dynamic Frequency Selection (DFS) requirements;
7. violate any accompanying user or technical manuals, training materials, specifications or other documentation pertaining to any Software, where in digital or printed format;
8. engage in any High Risk Activities (as defined in Section (V)(b)(ii));
9. release the results of any performance or functional evaluation of any of the Software to any third party without prior written approval of Ubiquiti for each such release; or
10. create a substantially similar software to the Software, or any component thereof.

iii. You are responsible for obtaining, properly installing and maintaining the Software and any other services or products needed for access to and use of the Software, and for paying all charges related thereto.

c. **Third Party Software**.

i. Certain software included in, distributed with or downloaded in connection with the Software may comprise third party proprietary software products that are subject to separate license terms ("**Third Party Software**"). All such Third Party Software may include

software or software components that are derived, in whole or in part, from software that is distributed as free software, open source software or under similar licensing or distribution models ("**Open Source Software**," together with Third Party Software, "**External Software**").

ii. Your use of External Software is subject in all cases to the applicable licenses from the External Software provider, which shall take precedence over the rights and restrictions granted in this EULA solely with respect to such External Software. You shall comply with the terms of all applicable Third Party Software and Open Source Software licenses, if any. Copyrights to Open Source Software are held by their respective copyright holders indicated in the copyright notices in the corresponding source files. The Software may include software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

iii. FOR THE AVOIDANCE OF DOUBT, UBIQUITI PROVIDES NO REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS, IMPLIED OR STATUTORY, WITH RESPECT TO SUCH EXTERNAL SOFTWARE, INCLUDING WITH RESPECT TO FUNCTIONALITY OF SUCH EXTERNAL SOFTWARE. Ubiquiti does not provide any warranty, maintenance, technical or other support for any External Software. Accordingly, Ubiquiti is not responsible for Your use of any External Software or any personal injury, death, property damage (including, without limitation, to Your home), or other harm or losses arising from or relating to Your use of any External Software.

d. **Intellectual Property Ownership; Trade Secrets.** All copyrights, trade secrets, patents, trademarks, trade secrets and other intellectual property and proprietary rights in any jurisdiction worldwide (collectively, "**Intellectual Property Rights**") in and to the Software and the Content are the sole property of Ubiquiti or its licensors. You do not have or receive any title or interest in or to the Software, the Content, or the Intellectual Property Rights contained therein through Your use of the Software or otherwise. Except as expressly granted to You under the limited license set forth in Section II(a) of this EULA, Ubiquiti does not grant any express or implied right to You under any of its Intellectual Property Rights. You further acknowledge and agree that the Software contains the valuable trade secrets and proprietary information of Ubiquiti and its affiliates. You agree to hold such trade secrets and proprietary information in confidence and You acknowledge that any actual or threatened breach of this obligation will constitute immediate, irreparable harm for which monetary damages would be an inadequate remedy, and that injunctive relief is an appropriate remedy for such breach.

e. **Trademarks.** All trademarks, service marks, trade names and logos and the goodwill associated therewith ("**Marks**") included or displayed in the Software or Content are the exclusive property of Ubiquiti or their respective holders. You are not permitted to use any of the Marks without the applicable prior written consent of Ubiquiti or such respective holders.

III. Automatic Updates.

a. Ubiquiti may, from time to time and at its sole option, provide patches, bug fixes, corrections, updates, upgrades, support and maintenance releases or other modifications to the Software,

including certain External Software, which items shall be deemed part of the Software and External Software hereunder. YOU HEREBY CONSENT TO ANY SUCH AUTOMATIC UPDATES. These may be automatically installed without providing any additional notice to You or receiving Your additional consent. If You do not consent, Your remedy is to stop using the Software. Notwithstanding the foregoing, Ubiquiti withholds the right to require You to install any patches, bug fixes, corrections, updates, upgrades, support and maintenance releases or other modifications in order to access and use the Software.

IV. Term and Termination. This EULA will remain in full force and effect so long as You continue to access or use the Software, or until terminated in accordance with this EULA. You may discontinue Your use of and access to the Software at any time. Ubiquiti will automatically terminate this EULA at any time without notice to you if you fail to comply with any term of this EULA. You may terminate it at any time upon written notice to Ubiquiti at legal@ubnt.com. Upon any such termination, the licenses granted by this EULA will immediately terminate and you agree to stop all access and use of the Product, Software and documentation and destroy the Software and documentation, together with all copies and merged portions in any form. The provisions that by their nature continue and survive will survive any termination of this EULA, including those set forth in this Sections II(d), II(e) and Articles IV -IX.

V. WARRANTY DISCLAIMER

a. **Disclaimer of Warranties** TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE SOFTWARE IS LICENSED “AS-IS” AND “AS AVAILABLE”, WITH ALL FAULTS. UBIQUITI DOES NOT MAKE ANY WARRANTIES OR REPRESENTATIONS OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, WITH RESPECT TO ANY SOFTWARE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY, ACCURACY, QUALITY OF SERVICE OR RESULTS, AVAILABILITY, SATISFACTORY QUALITY, LACK OF VIRUSES, TITLE, FITNESS FOR A PARTICULAR USE OR NON-INFRINGEMENT, TO THE EXTENT AUTHORIZED BY LAW. ANY STATEMENTS OR REPRESENTATIONS ABOUT THE SOFTWARE AND ITS FEATURES OR FUNCTIONALITY AND ANY COMMUNICATION WITH YOU IS FOR INFORMATION PURPOSES ONLY, AND DOES NOT CONSTITUTE A WARRANTY OR REPRESENTATION. WITHOUT LIMITING THE FOREGOING, UBIQUITI EXPRESSLY DOES NOT WARRANT THAT THE CONTENT, OPERATION, OUTPUT OR IMPLEMENTATION OF THE SOFTWARE WILL: (I) MEET YOUR REQUIREMENTS; (II) BE UNINTERRUPTED, ERROR-FREE, ACCURATE, RELIABLE OR COMPLETE; (III) BE COMPATIBLE WITH YOUR HOME NETWORK, COMPUTER OR MOBILE DEVICE; (IV) OR THAT UBIQUITI OR ANY THIRD PARTY WILL RESOLVE ANY PARTICULAR SUPPORT REQUEST OR FIX ANY ERRORS OR THAT SUCH RESOLUTION WILL MEET YOUR REQUIREMENTS OR EXPECTATIONS. YOU SHALL BEAR THE ENTIRE RISK AS TO THE QUALITY AND THE PERFORMANCE OF THE SOFTWARE.

b. **Emergency Response; High Risk Activities.**

i. YOU ACKNOWLEDGE AND AGREE THAT THE SOFTWARE, WHETHER STANDING ALONE OR WHEN INTERFACED WITH PRODUCTS OR THIRD-PARTY PRODUCTS OR SERVICES, ARE NOT CERTIFIED FOR EMERGENCY RESPONSE, AND ARE NOT A THIRD-PARTY MONITORED EMERGENCY NOTIFICATION SYSTEM. MOBILE OR OTHER NOTIFICATIONS REGARDING THE STATUS OF THE SOFTWARE ARE NOT A SUBSTITUTE FOR A THIRD-PARTY MONITORED EMERGENCY NOTIFICATION SYSTEM. YOU AGREE THAT YOU WILL NOT RELY ON THE SOFTWARE FOR EMERGENCY RESPONSE OR ANY OTHER LIFE SAFETY OR CRITICAL PURPOSES.

ii. NEITHER THE SOFTWARE NOR ANY PRODUCT IS DESIGNED, MANUFACTURED OR INTENDED FOR THE OPERATION OF NUCLEAR FACILITIES, AIR TRAFFIC CONTROL, EMERGENCY RESPONSE, EMERGENCY AND SAFETY SERVICES, HEALTHCARE FACILITIES, HOSPITALS, LIFE SUPPORT SYSTEMS OR ANY MISSION CRITICAL ENVIRONMENT, WHERE THE USE OR FAILURE OF THE SOFTWARE COULD LEAD TO DEATH, PERSONAL INJURY OR ENVIRONMENTAL DAMAGE (COLLECTIVELY, "**HIGH RISK ACTIVITIES**"). YOU AGREE THAT YOU WILL NOT USE THE SOFTWARE FOR ANY HIGH RISK ACTIVITIES.

c. **Data Storage.** Ubiquiti is not responsible or liable for the deletion of or failure to store or process any information or other content provided by You or transmitted in the course of using the Software. You are solely responsible for securing and backing up such submissions.

d. **Versions.** You acknowledge and agree that the Software provided to You under this EULA may be in "beta" or test form, or otherwise not intended or completed for commercial use and may therefore contain errors, bugs or similar unstable characteristics not typical of commercially released items. Such characteristics may negatively affect the operation of previously installed software or equipment. You are advised to safeguard important data, to use caution and not to rely in any way on the correct functioning or performance of the software and accompanying materials. You acknowledge that the Software may be provided to You from time to time as a program participant solely for the purpose of providing Ubiquiti with feedback on the Software and the identification of defects.

VI. LIMITATION OF LIABILITY

a. UNDER NO CIRCUMSTANCES WILL UBIQUITI OR ITS SUPPLIERS OR THEIR RESPECTIVE AFFILIATES, OFFICERS, EMPLOYEES, DIRECTORS, SHAREHOLDERS, AGENTS OR LICENSORS BE LIABLE UNDER ANY THEORY OF LIABILITY (WHETHER IN CONTRACT, TORT, STATUTORY OR OTHERWISE) FOR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF MONEY, REVENUES, PROFITS, GOODWILL, USE, DATA OR OTHER INTANGIBLE LOSSES (EVEN IF SUCH PARTIES WERE ADVISED OF, KNEW OF OR SHOULD HAVE KNOWN OF THE POSSIBILITY OF SUCH DAMAGES), RESULTING FROM THIS EULA OR THE INSTALLATION, MAINTENANCE, PERFORMANCE, FAILURE OR INTERRUPTION OR USE OF

SOFTWARE, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY (INCLUDING, WITHOUT LIMITATION, NEGLIGENCE), EVEN IF UBIQUITI HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IF, NOTWITHSTANDING THESE TERMS, UBIQUITI OR ANY OF ITS SUPPLIERS ARE FOUND TO BE LIABLE, THE LIABILITY OF UBIQUITI OR ITS SUPPLIERS OR THEIR RESPECTIVE AFFILIATES, OFFICERS, EMPLOYEES, DIRECTORS, SHAREHOLDERS, AGENTS OR LICENSORS TO YOU OR TO ANY THIRD PARTY IS LIMITED TO ONE HUNDRED DOLLARS ($100). THIS LIMITATION IS CUMULATIVE AND WILL NOT BE INCREASED BY THE EXISTENCE OF MORE THAN ONE INCIDENT OR CLAIM.

b. **Exclusions and Limitations.** Some jurisdictions do not allow the exclusion of certain warranties or the limitation or exclusion of liability for certain damages. Accordingly, some of the above limitations and disclaimers may not apply to You. To the extent that Ubiquiti may not, as a matter of applicable law, disclaim any implied warranty or limit its liabilities, the scope and duration of such warranty and the extent of Ubiquiti's liability will be the minimum permitted under such applicable law.

VII. INDEMNIFICATION. YOU AGREE TO INDEMNIFY, DEFEND, AND HOLD HARMLESS UBIQUITI AND ITS LICENSORS AND SUPPLIERS, AND THEIR RESPECTIVE AFFILIATES, OFFICERS, EMPLOYEES, DIRECTORS, SHAREHOLDERS, AGENTS OR LICENSORS FROM AND AGAINST ANY AND ALL CLAIMS, LIABILITIES, DAMAGES, LOSSES, COSTS, EXPENSES AND FEES (INCLUDING REASONABLE ATTORNEYS' FEES) THAT SUCH PARTIES MAY INCUR AS A RESULT OF OR ARISING FROM A VIOLATION OF THIS EULA.

VIII. Export Restrictions.

a. You acknowledge that the Software is of U.S. origin. You represent and warrant that (i) You shall be solely responsible for complying with all export laws and restrictions and regulations, including United States export regulations, such as restrictions of the Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control ("**OFAC**") or other foreign agency or authority's regulations ("**Export Laws**"), and You shall not (ii) export, or allow the export or re-export of, the Software in violation of any such restrictions, laws or regulations, or available in any country in contravention of any Export Laws, or any other law, nor (iii) make the Software available in a country for which an export license or other governmental approval is required without first obtaining all necessary licenses or other approvals. You shall obtain and bear all expenses relating to any necessary licenses and exemptions with respect to the export from the U.S. of the Software to any location.

b. You acknowledge that the U.S. government maintains embargoes and sanctions against certain countries, currently including the Crimea region of Ukraine, Cuba, Iran, North Korea, Sudan and Syria, which may be amended from time to time, including with respect to listed countries; and that other countries may have trade laws pertaining to import, use, export or distribution of the Software. You acknowledge that, in each case, compliance with the same is Your responsibility. You represent and warrant that You are not a person or entity listed on any United States Government list of prohibited or restricted parties.

IX. Miscellaneous.

a. **Governing Law; Jurisdiction.** This EULA shall not be governed by the 1980 U.N. Convention on Contracts for the International Sale of Goods; rather, this EULA shall be governed by the laws of the State of New York, including its Uniform Commercial Code, without reference to conflicts of laws principles. Any action or proceeding relating to this EULA must be brought in a federal or state court located in New York and each party irrevocably submits to the jurisdiction and venue of any such court in any such claim or dispute, except that Ubiquiti may seek injunctive relief in any court having jurisdiction to protect its confidential information or intellectual property.

b. **Government Purposes.** The Software was developed solely at private expense and is a "commercial item" consisting of "commercial computer software" and "commercial computer software documentation" within the meaning of the applicable civilian and military Federal acquisition regulations and any supplements thereto, as amended from time to time. If the user of the Software is an agency, department, employee or other entity of the United States Government, consistent with 48 C.F.R. 227.7202-1 through 227.702-4 (JUNE 1995), the use, duplication, reproduction, release, modification, disclosure and transfer of the Software, including technical data or manuals, is governed by the terms and conditions contained in this EULA.

c. **Severability.** If any of the provisions, either in part or in full, of this EULA is held by a court or other tribunal of competent jurisdiction to be unenforceable or invalid, such provision shall be enforced to the maximum extent possible or permissible and this EULA will be interpreted so as to give maximum effect to the original intent of the parties with respect to the unenforceable provision, and the remaining portions of this EULA shall remain in full force and effect.

d. **Assignment.** You may not assign any of Your rights or obligations under this EULA without Ubiquiti's express written consent. Ubiquiti may assign this EULA without Your consent provided that such assignment is to an affiliated company forming part of the Ubiquiti group of companies.

e. **Waiver.** The waiver by either party of any default by the other party shall not waive subsequent defaults by such other party of the same or different kind. The failure of either party to enforce the provisions hereof, at any time or for any period of time, or the failure of either party to exercise any option herein, shall not be construed as a waiver of such provision or option and shall in no way affect that party's right to enforce such provisions or exercise such option.

f. **Third Party Beneficiary.** Licensors and suppliers of Ubiquiti and its affiliates are third party beneficiaries of this EULA, and thus this EULA is directly enforceable by such licensors and suppliers and their affiliates.

g. **Statute of Limitations.** You agree that regardless of any statute or law to the contrary, any claim or cause of action You may have arising out of or related to use of the Software or this EULA must be filed within one (1) year after such claim or cause of action arose or be forever barred.

h. **Interpretation.** As used herein, unless the context requires otherwise, the word "or" is not exclusive and the words "will," "will not," "shall," and "shall not" are expressions of command and

not merely expressions of future intent or expectation. Whenever the words “include,” “includes” or “including” are used in this EULA, they shall be deemed to be followed by the words “without limitation.” The section headings in this EULA are for convenience only and have no legal or contractual effect.

STAY IN TOUCH

Email Address

SUBSCRIBE

Terms of Service | Privacy Policy | Legal

Exhibit D

Cambium Networks

ePMP | elevate

Quick Start Guide

Introduction and Concept

Migration Steps

Warranty and Support

Capabilities and Specifications

Introduction and Concept

ePMP™ Elevate allows the network operator, by remotely or locally software upgrading each ePMP Elevate-compatible subscriber device and installing an ePMP 1000 or *e*PMP 2000 access point, to receive substantial network performance and scalability benefits without requiring new subscriber hardware or physical installations. This Quick Start Guide provides guidance through the preparation and migration process using ePMP Elevate.

Migration Step 1: Review the ePMP Elevate Prerequisite Checklist

Please reference the information in this section to ensure a smooth ePMP Elevate migration experience.

Caution! *The ePMP Elevate migration process does require a brief system outage during access point transition. Please plan migration windows appropriately to minimize customer impact. Careful preparation and device pre-configuration will reduce resultant system downtime.*

3RD-PARTY SUBSCRIBER MODULE REQUIREMENTS/ACTIONS

- ☐ **Verify that your subscriber device is ePMP Elevate-compatible.**
  Visit the **ePMP Elevate website** for an up-to-date listing of ePMP Elevate-compatible 802.11n devices. All subscriber devices must be capable of 3rd-party software (ePMP Elevate) installation. *e*PMP Elevate devices may operate only as subscriber modules. ePMP Elevate does not support device operation in point-to-point, access point, or standard Wi-Fi modes.
- ☐ **Verify that your subscriber native software version is supported**
  XM/XW software version 5.6.6 is recommended. Other software versions not officially tested.
- ☐ **Verify/configure your current network's Network Mode.**
  If your current network is operating in **Router** mode, the network must be configured to operate in **Bridge** mode prior to ePMP Elevate transition.
- ☐ **Verify/configure your current network's Channel Size**.
  All subscribers must be configured with a channel width of **10 MHz**, **20 MHz**, or **40 MHz** prior to ePMP Elevate transition.
- ☐ **Record all subscriber RSSI (Received Signal Strength Indicator) and SNR (Signal-to-Noise Ratio) metrics prior to transition.**

FREQUENCY SUPPORT AND REGULATORY CERTIFICATIONS

Upgraded ePMP Elevate subscriber modules support operation in the frequency range 5150 – 5980 MHz. Upon upgrading to ePMP Elevate subscribers will be configured to scan all available frequencies to facilitate network entry.

Caution!

The user must ensure that deployed ePMP products operate in accordance to local regulatory limits. ePMP and ePMP Elevate-compatible devices may not share regulatory certifications in all regions.

Some 3rd-party radio devices were originally FCC-certified and labeled to operate in the 5.8 GHz frequency range only. An ePMP Elevate upgrade enables 3rd-party radios to operate within the U-NII-1 through U-NII-4 frequency band range 5150 – 5980 MHz. To ensure FCC regulatory compliance for ePMP Elevate-upgraded radio devices:

1. A new label must be applied to the device with the updated FCC ID clearly visible. 3rd-party radio manufacturers support FCC label requests online (labels are shipped directly).
2. FCC-allowed transmit power in the 5.8 GHz band has been reduced with the latest regulatory guidelines. ePMP Elevate adheres to these FCC power limits, and an upgrade to ePMP Elevate software may introduce a reduction of the device's operating transmit power to adhere to regulatory limits (as a result of the ePMP access point's transmit power control mechanism).

Although the access point does dynamically control subscriber output power, the subscriber's configured transmit power parameter is not altered upon upgrade.

This potential reduction of transmit power may have an impact on your network's radio link budgets. Cambium Networks' LINKPlanner tool allows operators to model link scenarios based on transmit power, geography, distance, antenna height, and other factors.

Migration Step 2: Pre-configure the ePMP access point for deployment

To ensure a quick subscriber transition of ePMP Elevate devices to the ePMP access point, follow the procedure below to pre-configure the ePMP access point.

ACCESS POINT PRE-CONFIGURATION EQUIPMENT AND TOOLS

- ☐ ePMP 1000 or ePMP 2000 connectorized access point connected to PoE power supply port "Gigabit Data+Power" by Ethernet cable
- ☐ PC connected to PoE power supply port "Gigabit Data" by Ethernet cable
- ☐ Power Supply powered on
- ☐ Supported browser – Chrome v29, Firefox v24, Internet Explorer 10, Safari v5 or later

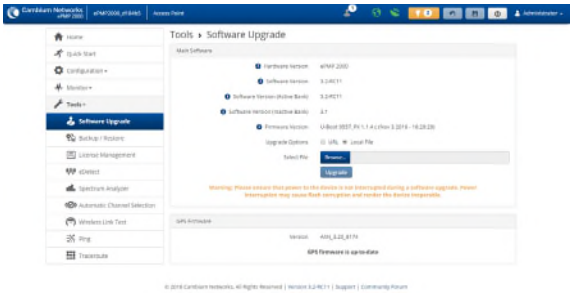
ACCESS POINT PRE-CONFIGURATION PROCEDURES

To ensure a quick subscriber transition of ePMP Elevate devices to the ePMP access point, follow the procedure below to pre-configure the ePMP access point.

Access Point software upgrade

To support registration from ePMP Elevate subscribers, the ePMP must be running ePMP Software Release 3.2 or later.

1. Download ePMP Software Release 3.2 (or later) from the Cambium Support website. For example, the Software Release 3.2 software package is named **ePMP-GPS_Synced-v3.2.tar.gz**.
2. Using a web browser, navigate to the access point's default IP address **192.168.0.1.**
3. Login to the access point web management interface with username: `admin` and password: `admin`.
4. Navigate to **Tools** > **Software Upgrade** and click the **Browse…** button to select the software release file downloaded in step 1.
5. Click **Upgrade**, then click the **Reboot Device** button.

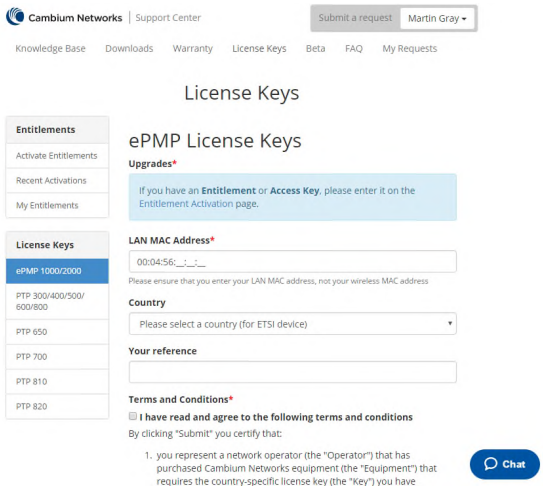


Access Point license generation and installation

To support registration from ePMP Elevate subscribers, the ePMP 1000/2000 access point must be configured with the appropriate licensing. ePMP Elevate entitlement IDs are emailed to operators by Cambium Networks distributors. The entitlement ID is used to generate a license key which is copied from the Cambium Networks License Key website and pasted to the ePMP access point to unlock ePMP Elevate functionality.

Generate license via the Cambium Networks License Keys website

1. Navigate to the Cambium Networks Entitlement Activation website.
2. Enter your entitlement IDs and click

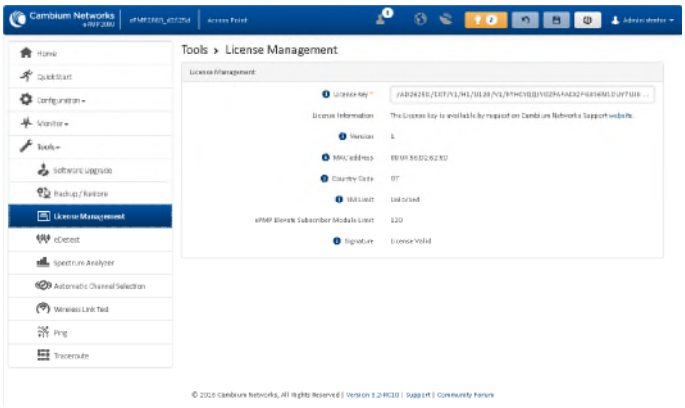


Check. Applicable entitlements are displayed below.

3 Click **Activate** to enact your entitlement.
4 Navigate to the Cambium Networks **ePMP License Keys website**.
5 Enter the **LAN MAC Address** of the ePMP access point.
6 Read the terms and conditions then acknowledge agreement by ticking the corresponding checkbox.
7 Click **Request Key**. An alphanumeric key is displayed below.
8 Copy the license key to the clipboard (Ctrl-C).

Enter the ePMP Elevate license key on the ePMP access point

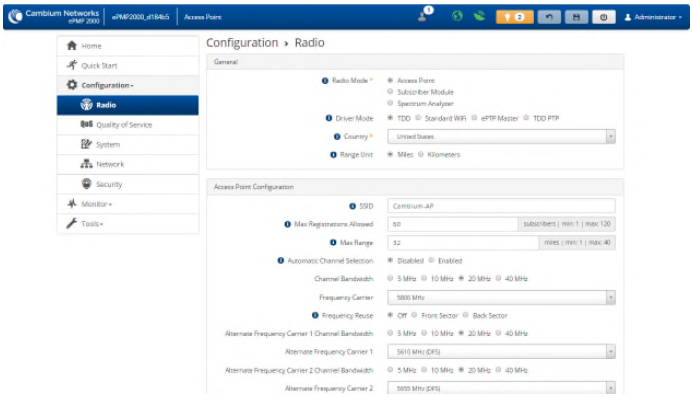
1 Using a web browser, navigate to the access point's default IP address **192.168.0.1**.
2 Login to the access point web management interface with username: `admin` and password: `admin`.
3 In the access point web management interface, navigate to **Tools > License Management**.
4 Paste the provided license key in field **License Key**.



Configure additional ePMP access point parameters per your network deployment

1 Using the ePMP access point web management interface, configure all applicable radio, QoS (Quality of Service), system, networking, and security parameters.

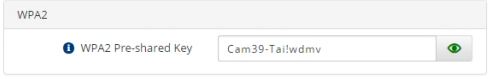
Note
After upgrade, ePMP Elevate subscribers retain only their configured **IP Address** and **Device Name**. All other parameters, including configured access point SSIDs, frequency configuration, VLAN, etc. must be configured after upgrade to ePMP Elevate.



2 Verify access point basic security parameters:
- **Wireless Security** is set to **Open** or **WPA2**, and
- **WPA2 Security Key** (if applicable) is configured to the system default of `Cam39-Tai!wdmv`

After upgrade, ePMP Elevate subscribers are configured with **Wireless Security** options **RADIUS** and **WPA2** enabled, meaning that both security options will be attempted upon network entry.

After upgrade ePMP Elevate subscribers are configured with the default ePMP **WPA2 Pre-shared Key** of `Cam39-Tai!wdmv`. If the ePMP access point has been configured with a new, non-default **WPA2 Pre-shared Key**, this key



must be configured on all network subscribers to allow network entry.

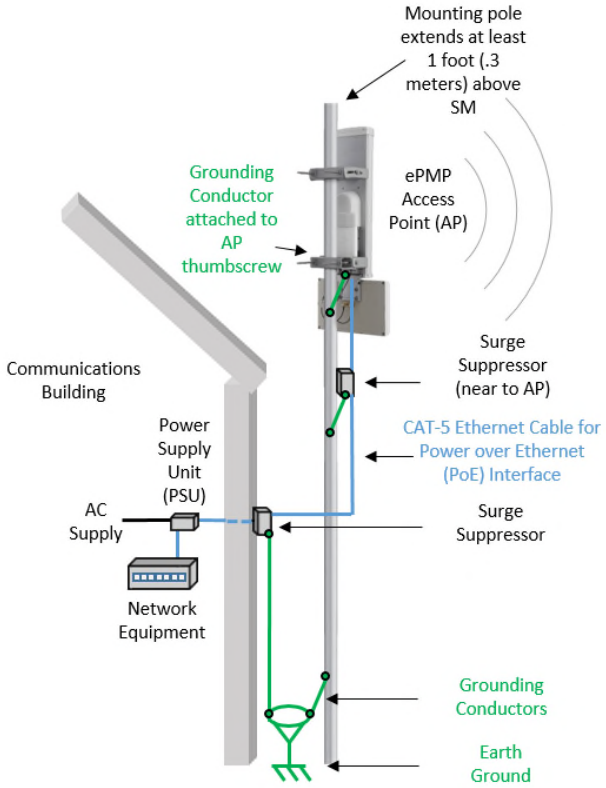
3 After configuring access point parameters, click **Save** then click the **Reboot** button.

Migration Step 3: Install and power on the ePMP access point on-site

For additional ePMP access point installation requirements, see the *ePMP User Guide*, available here: Cambium Support website.

Option 1 (Preferred): When possible, install the ePMP access point onsite after pre-configuration. This technique offers the best opportunity to minimize the network outage time required upon subscriber transition to the ePMP access point.

Option 2: Alternatively, the ePMP access point may be installed as a direct replacement to the currently operating access point using the same mounting equipment (when possible). This technique will require more subscriber downtime than option 1.



Migration Step 4: Upgrade ePMP Elevate-compatible subscribers

Installing the ePMP Elevate software on supported subscriber modules allows registration of the subscriber to the ePMP access point. This procedure may be completed remotely (over-the-air, does not require a site visit) or locally (via direct wired Ethernet connection to each subscriber module, requires a site visit).

Caution! *The ePMP Elevate migration process does require a brief system outage during access point transition. Once the ePMP Elevate software has been installed on a subscriber, it will no longer register to its original access point, and network entry will only be available via the ePMP access point. Please plan migration windows appropriately to minimize customer impact. Careful preparation and device pre-configuration will reduce resultant system downtime.*

SUBSCRIBER SOFTWARE UPGRADE TO EPMP ELEVATE

1 Download ePMP Elevate software (based on device type) from the Cambium Support website.
2 Using a web browser, navigate to the subscriber module's configured management IP address.
3 Login to the subscriber module using your configured username and password.
4 Upgrade the device software using the ePMP Elevate software package from Step 1.

5 Reboot the device.
The subscriber will now begin to scan all available frequencies and channel bandwidths for network entry via the installed ePMP access point.

Note
After upgrade, ePMP Elevate subscribers retain only their configured IP Address and Device Name. All other parameters, including configured access point SSIDs, frequency configuration, VLAN, etc. may be configured over-the-air after upgrade to ePMP Elevate.

SUBSCRIBER MODULE POST-UPGRADE NOTES

- After upgrade, the ePMP Elevate subscriber module may be accessed via its previously-configured management IP address.
- ePMP Elevate subscriber modules may be access via default username: `admin` and password `admin`.
- To reduce scan time at startup, it is recommended to configure only your primary and alternate frequencies / channel sizes. These may be configured on the ePMP Elevate subscriber's **Configuration** > **Radio** page
- After upgrade, the ePMP Elevate subscribers are configured by default to attempt network entry to the first ePMP access point scanned. To specify a specific access point SSID, configure the **Preferred APs** table (located on the ePMP Elevate subscriber's **Configuration** > **Radio** page) to match the SSID configuration on the deployed ePMP access point.

Migration Step 5: Power down original access point, power on ePMP access point

Caution! *This step will introduce a brief system outage as the ePMP Elevate subscribers are migrated to the ePMP access point*

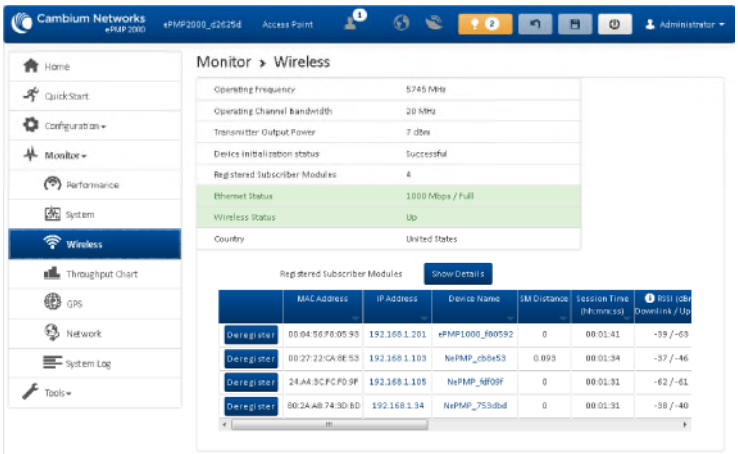
ACCESS POINT TRANSITION

1 Power down the existing access point. When possible, it is recommended to physically remove original access point equipment after verifying subscriber registration and link quality (Migration Step 6).
2 Power on the ePMP access point. After this step, the ePMP Elevate-upgraded subscribers will register to the ePMP access point.

Migration Step 6: Verify subscriber registration and link quality

EPMP ELEVATE SUBSCRIBER REGISTRATION VERIFICATION

1 Log into the ePMP access point web management interface.
2 On the access point **Home** page, verify that the **Registered Subscriber Modules** statistic displays the expected subscriber count.
3 Navigate to the access point **Monitor** > **Wireless** page and validate subscriber **RSSI** and **SNR** values. Updated FCC transmit power regulations may affect link budget, see Frequency Support and Regulatory Certifications.
4 To test wireless link data capacity, navigate to the access point page **Tools** > **Wireless Link Test**.



Migration Step 7: Remove original access point equipment

Once the ePMP link has been validated, the original access point equipment may be removed.

ePMP Elevate Warranty and Support

Cambium Networks supports software maintenance of ePMP Elevate, and ePMP Elevate subscribers are operated at the user's own risk. For ePMP Elevate software support after migration, visit the Cambium Networks Support Website.

Cambium Networks does not accept any liability for reliability or interface responsiveness of ePMP Elevate-compatible hardware upgraded with ePMP Elevate.

Cambium Networks does not accept any liability for hardware damage or replacement.

ePMP Elevate Capabilities and Specifications

The following table provides detail of ePMP Elevate operation after installation/upgrade:

Registration and Licensing	**Total Registration Capacity**	120 subscribers
	ePMP Elevate Subscriber Licensing	ePMP 1000/2000 access points support a maximum number of ePMP Elevate subscriber modules based on the purchased ePMP Elevate licensing.
	ePMP Subscriber Licensing	Cambium ePMP subscriber modules are not limited by licensing, and may be deployed up to the platform limit (120 subscribers, inclusive of upgraded ePMP Elevate subscriber modules).
	Additional ePMP Elevate Licensing	Additional licenses may be purchased and installed on the ePMP 1000/2000 access point to increase the capacity of supported ePMP Elevate subscribers.
Modes of Operation	**Scheduler Modes**	TDD (Time Division Duplex) and Flexible
	ePMP Elevate Subscriber Mode Support	ePMP Elevate devices may operate only as subscriber modules. ePMP Elevate does not support device operation in point-to-point, access point, or standard Wi-Fi modes.
Radio Operation	**Frequencies Supported**	5150 – 5980 MHz  Note The available spectrum for operation depends on the region. When configured with the appropriate country code, the unit will only allow operation on those channels which are permitted by the regulations.
	Channel Sizes Supported	5, 10, 20, 40 MHz
Device Management	**cnMaestro**	Inventory management, device onboarding, daily operations, and maintenance of ePMP Elevate subscriber modules and ePMP products is supported by cnMaestro cloud-based management software. ePMP Elevate subscriber modules may also be managed by other third-party Network Management/Element Management systems via the ePMP software SNMP protocol support.

Exhibit E

Cambium Networks

ePMP™

Release Notes

System Release 3.5.1

Sections included:

Introduction
Product Releases
Scope
Defect Fixes
Known Limitations
Technical Support
Community Forum

Introduction

This document provides information for the Cambium Networks ePMP Series System Release 3.5.1.

The information in this document is subject to change without notice. The recommendations, technical data, configurations and statements in this document are believed to be reliable and accurate, but are presented without implied or express warranty. Users must take full responsibility for their applications of any product specified in this document. The information in this document is proprietary to Cambium Networks Ltd.

Product Releases

Hardware

EPMP 2000

Part Number	Description
C050900A033A	ePMP 2000: 5 GHz AP with Intelligent Filtering and Sync (EU)
C058900A132A	ePMP 2000: 5 GHz AP with Intelligent Filtering and Sync (FCC)
C050900A031A	ePMP 2000: 5 GHz AP with Intelligent Filtering and Sync (ROW) (no cord)
C050900A231A	ePMP 2000: 5 GHz AP with Intelligent Filtering and Sync (ROW) (EU cord)
C050900A131A	ePMP 2000: 5 GHz AP with Intelligent Filtering and Sync (ROW) (US cord)
C050900A333A	ePMP 2000: 5 GHz AP with Intelligent Filtering and Sync (EU) (UK cord)
C050900A331A	ePMP 2000: 5 GHz AP with Intelligent Filtering and Sync (ROW) (UK cord)
C050900A431A	ePMP 2000: 5 GHz AP with Intelligent Filtering and Sync (ROW) (India cord)
C050900A531A	ePMP 2000: 5 GHz AP with Intelligent Filtering and Sync (ROW) (China cord)
C050900A631A	ePMP 2000: 5 GHz AP with Intelligent Filtering and Sync (ROW) (Brazil cord)
C050900A731A	ePMP 2000: 5 GHz AP with Intelligent Filtering and Sync (ROW)(Argentina cord)
C050900A831A	ePMP 2000: 5 GHz AP with Intelligent Filtering and Sync (ROW)(ANZ cord)
C050900L033A	ePMP 2000: 5 GHz AP Lite with Intelligent Filtering and Sync (EU)
C058900L132A	ePMP 2000: 5 GHz AP Lite with Intelligent Filtering and Sync (FCC)
C050900L031A	ePMP 2000: 5 GHz AP Lite with Intelligent Filtering and Sync (ROW) (no cord)
C050900L231A	ePMP 2000: 5 GHz AP Lite with Intelligent Filtering and Sync (ROW) (EU cord)
C050900L131A	ePMP 2000: 5 GHz AP Lite with Intelligent Filtering and Sync (ROW) (US cord)
C050900L333A	ePMP 2000: 5 GHz AP Lite with Intelligent Filtering and Sync (EU) (UK cord)

C050900L331A	ePMP 2000: 5 GHz AP Lite with Intelligent Filtering and Sync (ROW) (UK cord)
C050900L431A	ePMP 2000: 5 GHz AP Lite with Intelligent Filtering and Sync (ROW) (India cord)
C050900L531A	ePMP 2000: 5 GHz AP Lite with Intelligent Filtering and Sync (ROW) (China cord)
C050900L631A	ePMP 2000: 5 GHz AP Lite with Intelligent Filtering and Sync (ROW) (Brazil cord)
C050900L731A	ePMP 2000: 5 GHz AP Lite with Intelligent Filtering and Sync (ROW) (Argentina cord)

EPMP 1000

The following tables provides the key components available for purchase:

Part Number	Description
C050900A011A	ePMP 1000: 5 GHz Connectorized Radio with Sync (ROW)
C050900A013A	ePMP 1000: 5 GHz Connectorized Radio with Sync (EU)
C058900A112A	ePMP 1000: 5 GHz Connectorized Radio with Sync (FCC)
C050900A021A	ePMP 1000: 5 GHz Connectorized Radio (ROW)
C050900A023A	ePMP 1000: 5 GHz Connectorized Radio (EU)
C058900A122A	ePMP 1000: 5 GHz Connectorized Radio (FCC)
C050900C031A	ePMP 1000: 5 GHz Integrated Radio (ROW)
C050900C033A	ePMP 1000: 5 GHz Integrated Radio (EU)
C058900C132A	ePMP 1000: 5 GHz Integrated Radio (FCC)
C024900A011A	ePMP 1000: 2.4 GHz Connectorized Radio with Sync
C024900A021A	ePMP 1000: 2.4 GHz Connectorized Radio
C024900C031A	ePMP 1000: 2.4 GHz Integrated Radio

FORCE 110

Part Number	Description
C058900C042B	ePMP Force 110AR5-25 High Gain (25 dBi) SM/PTP Radio (FCC)
C050900C043B	ePMP Force 110AR5-25 High Gain (25 dBi) SM/PTP Radio (EU)
C050900C041B	ePMP Force 110AR5-25 High Gain (25 dBi) SM/PTP Radio (ROW)
C058900B052A	ePMP Force 110 PTP - High Performance PTP Radio (FCC)
C050900B053A	ePMP Force 110 PTP - High Performance PTP Radio (EU)
C050900B051A	ePMP Force 110 PTP - High Performance PTP Radio (ROW)

FORCE 180

Part Number	Description
C058900C072A	ePMP 5 GHz Force 180 Integrated Radio (FCC) (US cord)
C050900C071A	ePMP 5 GHz Force 180 Integrated Radio (ROW) (no cord)
C050900C073A	ePMP 5 GHz Force 180 Integrated Radio (EU) (EU cord)
C050900C171A	ePMP 5 GHz Force 180 Integrated Radio (ROW) (US cord)
C050900C271A	ePMP 5 GHz Force 180 Integrated Radio (ROW) (EU cord)
C050900C371A	ePMP 5 GHz Force 180 Integrated Radio (ROW) (UK cord)
C050900C373A	ePMP 5 GHz Force 180 Integrated Radio (EU) (UK cord)
C050900C471A	ePMP 5 GHz Force 180 Integrated Radio (ROW) (India cord)
C050900C571A	ePMP 5 GHz Force 180 Integrated Radio (ROW) (China cord)
C050900C671A	ePMP 5 GHz Force 180 Integrated Radio (ROW) (Brazil cord)
C050900C771A	ePMP 5 GHz Force 180 Integrated Radio (ROW) (Argentina cord)
C050900C871A	ePMP 5 GHz Force 180 Integrated Radio (ROW) (ANZ cord)

FORCE 190

Part Number	Description
C058900C082A	ePMP Force 190 5 GHz Subscriber Module (FCC) (US Cord)
C050900C083A	ePMP Force 190 5 GHz Subscriber Module (EU) (EU Cord)
C050900C873A	ePMP Force 190 5 GHz Subscriber Module (EU) (UK Cord)
C050900C081A	ePMP Force 190 5 GHz Subscriber Module (RoW) (No Cord)
C050900C181A	ePMP Force 190 5 GHz Subscriber Module (RoW) (US Cord)
C050900C281A	ePMP Force 190 5 GHz Subscriber Module (RoW) (EU Cord)
C050900C481A	ePMP Force 190 5 GHz Subscriber Module (RoW) (India Cord)
C050900C581A	ePMP Force 190 5 GHz Subscriber Module (RoW) (China Cord)
C050900C681A	ePMP Force 190 5 GHz Subscriber Module (RoW) (Brazil Cord)
C050900C781A	ePMP Force 190 5 GHz Subscriber Module (RoW) (Type-N Plug Cord)
C050900C881A	ePMP Force 190 5 GHz Subscriber Module (RoW) (ANZ Cord)
C050900C981A	ePMP Force 190 5 GHz Subscriber Module (RoW) (No PSU)

FORCE 200

Part Number	Description
C058900C062A	ePMP 5 GHz Force 200AR5-25 High Gain Radio (FCC) (US cord)
C050900C061A	ePMP 5 GHz Force 200AR5-25 High Gain Radio (ROW) (no cord)
C050900C063A	ePMP 5 GHz Force 200AR5-25 High Gain Radio (EU) (EU cord)
C050900C161A	ePMP 5 GHz Force 200AR5-25 High Gain Radio (ROW) (US cord)
C050900C261A	ePMP 5 GHz Force 200AR5-25 High Gain Radio (ROW) (EU cord)
C050900C361A	ePMP 5 GHz Force 200AR5-25 High Gain Radio (ROW) (UK cord)
C050900C363A	ePMP 5 GHz Force 200AR5-25 High Gain Radio (EU) (UK cord)
C050900C461A	ePMP 5 GHz Force 200AR5-25 High Gain Radio (ROW) (India cord)
C050900C561A	ePMP 5 GHz Force 200AR5-25 High Gain Radio (ROW) (China/ANZ cord)
C050900C661A	ePMP 5 GHz Force 200AR5-25 High Gain Radio (ROW) (Brazil cord)
C050900C761A	ePMP 5 GHz Force 200AR5-25 High Gain Radio (ROW) (Argentina cord)
C024900C161A	ePMP 2.4 GHz Force 200AR2-25 High Gain Radio (US cord)
C024900C261A	ePMP 2.4 GHz Force 200AR2-25 High Gain Radio (EU cord)
N000900L021A	ePMP Force 200 Radome

ACCESSORIES

Part Number	Description
C050900D021A	ePMP 2000/1000: 5 GHz Sector Antenna - 90° / 120°
C050900D020A	ePMP 2000: 5 GHz Smart Antenna
C050900D002A	ePMP 1000: 5 GHz Sector Antenna - 120°
C050900D003A	ePMP 1000: 5 GHz Sector Antenna - 90°
C024900D004A	ePMP 1000: 2.4 GHz Sector Antenna - 90° / 120°
N000900L001B	ePMP 1000: Spare Power Supply for Radio with Gigabit Ethernet (no cord)
N000900L002A	ePMP 1000: Spare Power Supply for Radio with 100Mbit Ethernet (no cord)
N000900L005A	ePMP 1000: Spare GPS Antenna
C050900H007B	4 pack of C050900D007B: ePMP 110A5-25 Dish Antenna (25 dBi) for ePMP Connectorized Radio

Embedded Software

RELEASE SOFTWARE

New ePMP software releases may be downloaded from the ePMP Downloads website.

The following software update is provided with ePMP System Release 3.5.1:

Device Description	Applicable Software Package
Connectorized Radio with Sync	ePMP-GPS_Synced-v3.5.1.tar.gz
Integrated Radio / Connectorized Radio	ePMP-NonGPS_Synced-v3.5.1.tar.gz
CNUT package (for all radios)	ePMP-3.5.1.pkg3

EPMP ELEVATE SOFTWARE

The following software is provided with ePMP Elevate in ePMP System Release 3.5.1:

Application Description	Applicable Software Package
ePMP Elevate (XM firmware devices) *Use this file if upgrading an XM device to ePMP Elevate for the first time*	UBNTXM-ubntxm-squashfs-factory.bin
ePMP Elevate (XW firmware devices) *Use this file if upgrading an XM device to ePMP Elevate for the first time*	UBNTXW-ubntxw-squashfs-factory.bin
ePMP Elevate (XM firmware devices)	UBNTXM-v3.5.1.tar.gz
ePMP Elevate (XW firmware devices)	UBNTXW-v3.5.1.tar.gz

SPECIAL SOFTWARE UPGRADE NOTICE

All users of ePMP product are encouraged to upgrade the Connectorized Radio with Sync, Integrated Radio, Connectorized Radio, Force 180, Force 190 and Force 200 units to the latest System Release 3.5.1. ePMP software updates can be downloaded from the **ePMP Downloads website**. For instructions on upgrading an ePMP device, see the *ePMP User Guide*.

Note

While upgrading a **Connectorized Radio with Sync** from the factory, ensure both the device software banks are updated. Upgrade to the latest software **TWICE** so that both Active & Backup are updated. This is NOT required for Integrated or Connectorized Radios since these radios do not have two software banks.

While upgrading devices with System Release 1.0.3 or earlier, ensure that the browser cache is cleared prior to the upgrade.

Caution

ePMP radios running System Release 2.1 or earlier cannot be directly upgraded to System Release 3.5.1. Please upgrade to System Release 2.6 first, then upgrade to System Release 3.5.1. Stepping through System Release 2.6 is not required if the ePMP radio is running System Release 2.2 or later.

UPGRADING THE ON-BOARD GPS CHIP FIRMWARE

Beginning with System Release 2.0, users can upgrade the firmware of the on-board GPS chip present on the **Connectorized Radio with Sync**. All users are strongly encouraged to upgrade the on-board GPS chip firmware in order to avoid sporadic lock up of the chip during normal operation. ePMP software updates can be downloaded from the **ePMP Downloads website**.

GPS Chip and Software Reference

	ePMP 1000 (1st Generation)	ePMP 1000 (2nd Generation)	ePMP 2000
GPS Chip Type	GPS only	GPS + GLONASS	GPS + GLONASS
Default GPS Firmware	AXN_1.51_2801	AXN_3.20_8174	AXN_3.20_8174
Potential Issues (With Default Firmware Installed)	GPS chip locked, resulting in loss of sync and no display of firmware version or visible/tracked satellites	Occasional sync loss following low number of tracked satellites for customers in APAC and Russia regions	Occasional sync loss following low number of tracked satellites for customers in APAC and Russia regions
Current GPS Firmware	AXN_1.51_2838	AXN_5.1._8174	AXN_5.1._8174
Corresponding ePMP Software Release	2.1	3.5.1	3.5.1
Known issues (With Current GPS Firmware)	None	None	None

For instructions on upgrading the GPS chip firmware, see below or refer the *ePMP User Guide*.

To upgrade the on-board GPS chip on a Connectorized Radio with Sync (1st Generation - purchased 2015 and prior):

1. Navigate to **Monitor > GPS** to check the **GPS Firmware Version** that is currently present on the radio.
2. If the GPS Firmware Version displays **AXN_1.51_2838** and/or "**GPS Firmware is up-to-date**", do nothing. The on-board GPS chip already has the latest firmware.
3. If the GPS Firmware Version displays **AXN_1.51_2801**, navigate to **Tools > Software** Upgrade page.
4. Under the **GPS Firmware** upgrade section, select the same package used to upgrade the device's firmware ex: **ePMP-GPS_Synced-v3.5.1.tar.gz.**
5. Click the **Upgrade** button.
6. The upgrade can take up to 3 minutes. Once the upgrade is done, the radio's UI prompts for a reboot and the reboot button will be highlighted.
7. Click the Reboot button on the top right corner of the UI.
8. Once the radio has completed its reboot process, check under the **Monitor > GPS** page to ensure that the **GPS Firmware Version** displays **AXN_1.51_2838.**

To upgrade the on-board GPS chip on a Connectorized Radio with Sync (2nd Generation - purchased 2016 and after):

1. Navigate to **Monitor > GPS** to check the **GPS Firmware Version** that is currently present on the radio.
2. If the GPS Firmware Version displays **AXN_5.1_8174** and/or "**GPS Firmware is up-to-date**", do nothing. The on-board GPS chip already has the latest firmware.
3. If the GPS Firmware Version displays **AXN_3.20_8174**, navigate to **Tools > Software** Upgrade page.
4. Under the **GPS Firmware** upgrade section, select the same package used to upgrade the device's firmware ex: **ePMP-GPS_Synced-v3.5.1.tar.gz.**
5. Click the **Upgrade** button.
6. The upgrade can take up to 3 minutes. Once the upgrade is done, the radio's UI prompts for a reboot and the reboot button will be highlighted.
7. Click the Reboot button on the top right corner of the UI.
8. Once the radio has completed its reboot process, check under the **Monitor > GPS** page to ensure that the **GPS Firmware Version** displays **AXN_5.1_8174.**

 Note

On occasion the **GPS Firmware Version** under **Monitor > Tools** may display **NA**. This means that the GPS chip has already locked up and is no longer communicating with the main processor. Perform a hard reboot (power cycle the entire unit) to restore communication. Then perform steps 3 through 8 above.

This is NOT required for Integrated or Connectorized Radios since these radios do not have an on-board GPS chip.

NEW LOCAL IP

Prior to System Release 2.1, in both Bridge and NAT mode, the ePMP Device was previously accessible through a local IP of 10.1.1.254 through the LAN port. Beginning with System Release 2.1, the local IP has been updated to **169.254.1.1(/16).**

EPMP POST-UPGRADE IP ADDRESSING

If **Device IP address Mode** is set to **DHCP** and the device is unable to retrieve IP address information via DHCP, the device management IP is set to fallback IP of *192.168.0.1* (AP mode), *192.168.0.2* (SM mode), *192.168.0.3* (Spectrum Analyzer mode) or a previously configured static Device IP Address. Units can always be accessed via the Ethernet port with a local IP of *169.254.1.1*.

SPECTRUM ANALYZER ON SM WHEN USING PORT FORWARDING OR DMZ

If port forwarding or DMZ is enabled on the SM, it is necessary to add a port forwarding entry for the Spectrum Analyzer to work. The Spectrum Analyzer uses port 8001 and this must be explicitly added in the port forwarding table under **Configure>Network>NAT>Advanced**, on the radio's GUI. In addition, once the Spectrum Analyzer is launched on the client PC, select the Port Forwarding IP as the device IP address under **Tools>Preferences**, on the Spectrum Analyzer Java tool. Depending on the network configuration, the generation configuration scheme must be **Client PC > Port_Forwarding_IP:8001 > Device_IP:8001.**

SPECTRUM ANALYZER WHEN MANAGEMENT VLAN IS ENABLED

When Management VLAN is enabled on the ePMP radio, the Spectrum Analyzer client must be launched from the same network as the Management VLAN.

CHROME / FIREFOX WEB MANAGEMENT INTERFACE ACCESS – SPECIAL NOTICE FOR SOFTWARE RELEASE 3.4 / 3.4.1

If access to the web management interface is lost after upgrading to Software Release 3.4 or 3.4.1, it is recommended to clear the browser cookies and cache to regain access. This workaround is only applicable to devices which have been loaded with Software Release 3.4 or 3.4.1.

Instructions for clearing cookies / cache in Google Chrome:
https://support.google.com/accounts/answer/32050?co=GENIE.Platform%3DDesktop&hl=en

Instructions for clearing cookies / cache in Mozilla Firefox:
https://support.mozilla.org/en-US/kb/delete-cookies-remove-info-websites-stored

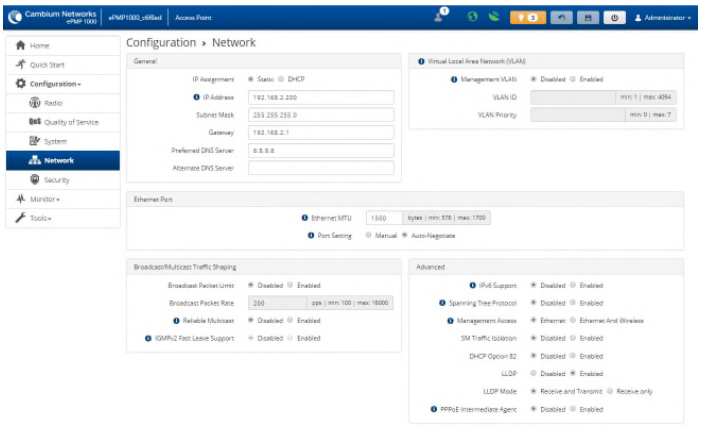
cnMaestro™

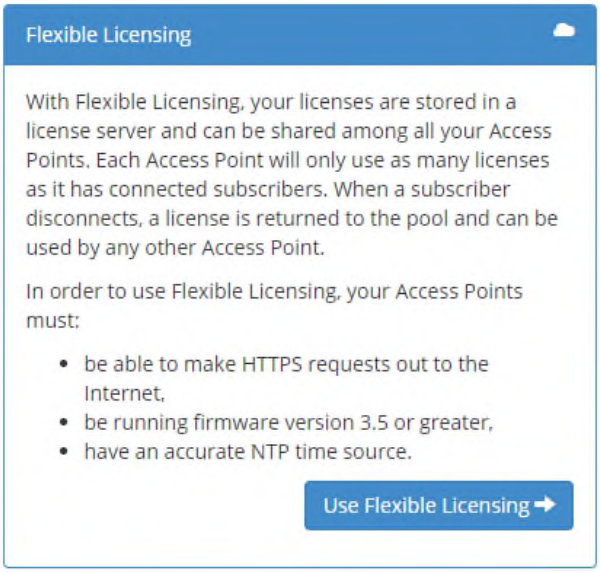
*cn*Maestro is a cloud-based or on-site platform designed to monitor, configure, operate, upgrade, manage and monitor ePMP systems. For more information, see the cnMaestro website.

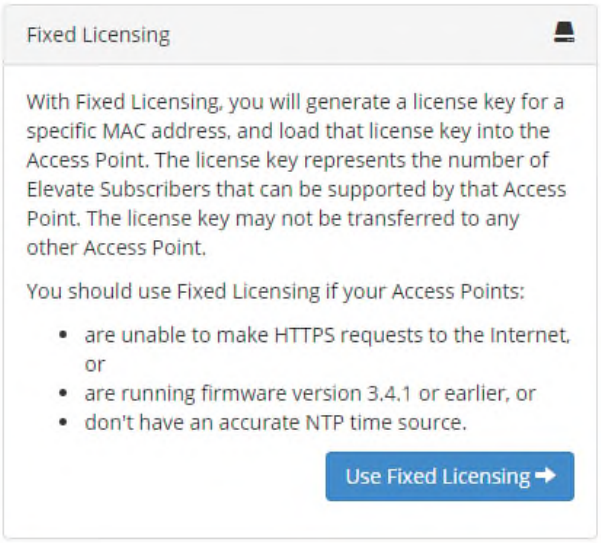
New Features

ePMP Elevate Floating License Server Official Release

Software Release 3.5.1 introduces official support for the ePMP Elevate Floating License Server functionality. There are two types of ePMP Elevate license management mechanisms available on the ePMP device – Flexible and Fixed, as described below:







The AP's **License Management** page is used to:

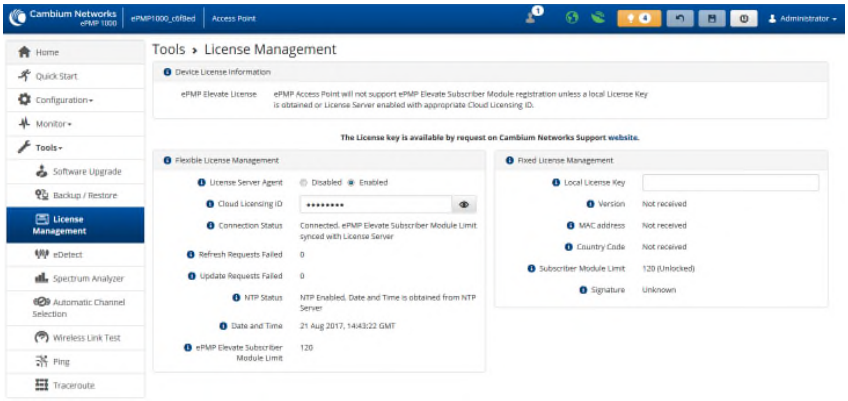
- Install licensing for ePMP Elevate subscriber access allotments
- Convert the AP from Lite (10 subscriber) to Full (120 subscriber)
- Configure the Country Code ETSI-locked devices

Note

ePMP 3.4.1 and earlier Releases support only Fixed Licensing.

Elevate Flexible Licensing is available only for ePMP AP devices with GPS sync.

Country Code configuration for ETSI locked device and Full Capacity Keys for AP Lite devices are available only via Fixed License Management. Elevate is available via Fixed or Flexible License Management.



Note

To use flexible licensing, the AP must:

1. be able to make HTTPS requests out to the Internet
2. be running firmware version 3.5.1 or greater
3. have an accurate NTP time source

AP web management interface flexible licensing parameters:

Attribute	Meaning
Flexible License Management	
License Server Agent	Disabled: No communication with the License Server is established Enabled: Enables License Server functionality to obtain the number of allowed ePMP Elevate SMs to be connected to the AP
Cloud Licensing ID	This field represents a Cambium Networks customer identification used for AP identification on the License Server. This identifier is generated upon License Entitlement activation at the Cambium Networks web-based Support Center.
Connection Status	The **Connection Status** displays the License Server process state when **License Server Agent** is **Enabled**. This status may also be referenced on the device **Home** page.
Refresh Requests Failed	The number of failed refresh (polling) requests to the License Server. The **ePMP Elevate Subscriber Module Limit** resets to 1 after the 3rd failed refresh request.
Update Requests Failed	The number of failed update (licensing information transfer) requests to the License Server. The **ePMP Elevate Subscriber Module Limit** resets to 1 after the 5th failed updated request.
NTP Status	Represents whether or not the current time and date have been retrieved from the configured NTP server
ePMP Elevate Subscriber Module Limit	The number of ePMP Elevate devices allowed to register to the AP

FLEXIBLE LICENSE GENERATION PROCEDURE

Procedure:

Follow this procedure to set up the Cambium Networks licensing portal to host ePMP Elevate licenses:

1 Purchase the desired license product Entitlements from your Cambium Networks distributor (C050900S510A – 10 ePMP Elevate licenses)

2 Cambium Networks will email your Entitlements to the provided email address. An example of the email is displayed below:

Cambium Networks is pleased to deliver an Entitlement Certificate that you may use to redeem your recent purchase of software license key(s). To redeem this entitlement, please go to the Cambium Support Center and follow the instructions. If you need any assistance with this process, please contact Cambium Networks Support by phone or support@cambiumnetworks.com.

Entitlement Details

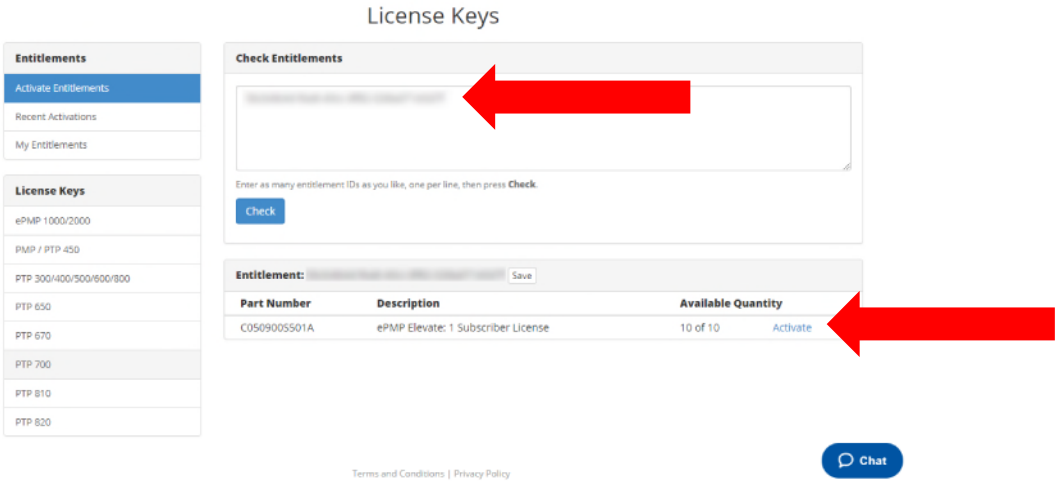
Entitlement ID:	[redacted]	**Start Date:**	08/04/2017
Company:		**End Date:**	Never expires
Contact:	[redacted]		
Cambium Order Reference:			
Your Order Reference:			

Associated Products

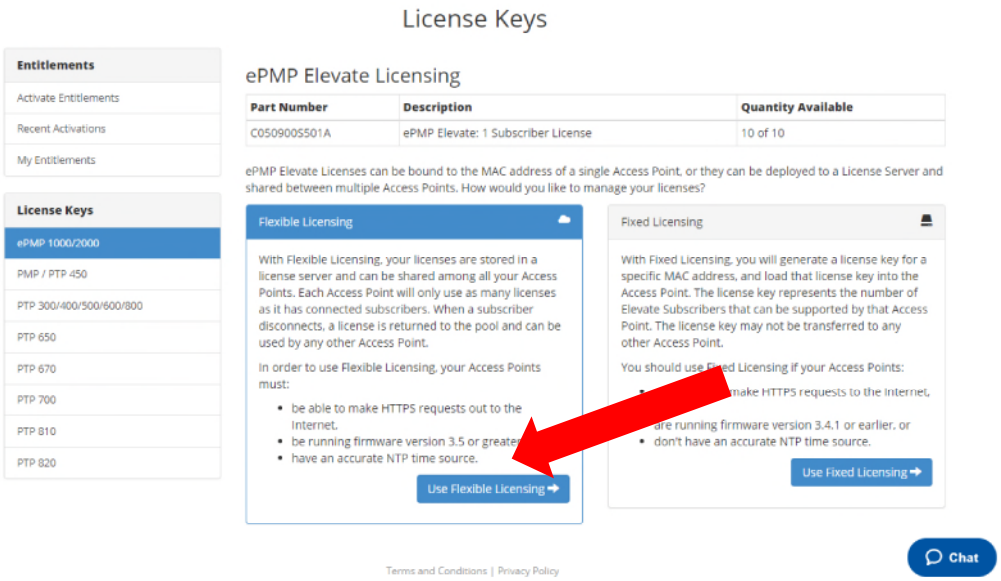
Product Number	Description	Quantity Ordered	Remaining Quantity
C050900S501A 1	ePMP Elevate: 1 Subscriber License	200	200
C050900S510A 1	ePMP Elevate: 10 Subscriber License	5	5

Cambium Networks Support

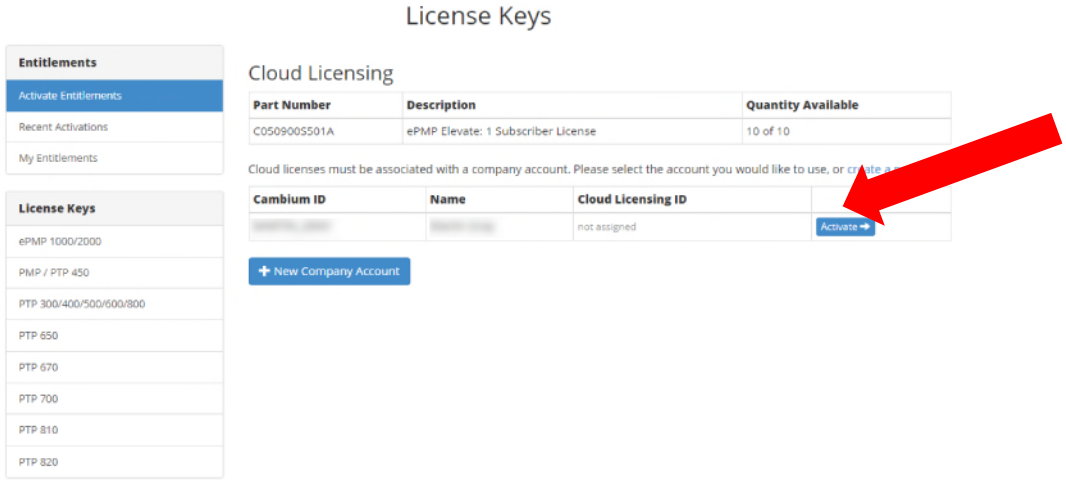
3 Log into support.cambiumnetworks.com/licensekeys and navigate to **Activate Entitlements**. Enter your provided **Entitlement ID** in the **Check Entitlements** section and click the **Check** button. Entitlement details are listed in the dialogue below. Click **Activate** to activate the Entitlement's corresponding licenses.



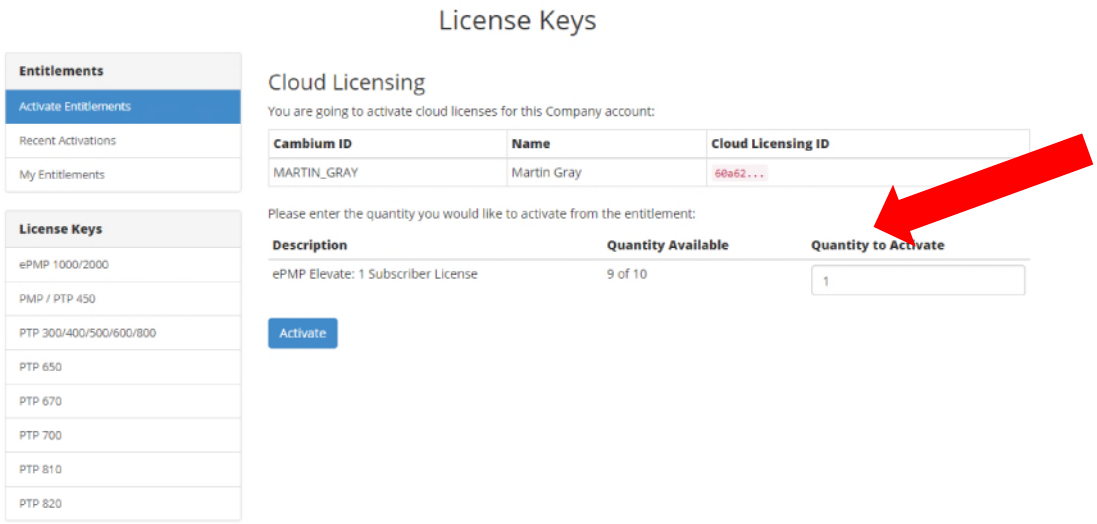
4 Select **Use Flexible Licensing.**



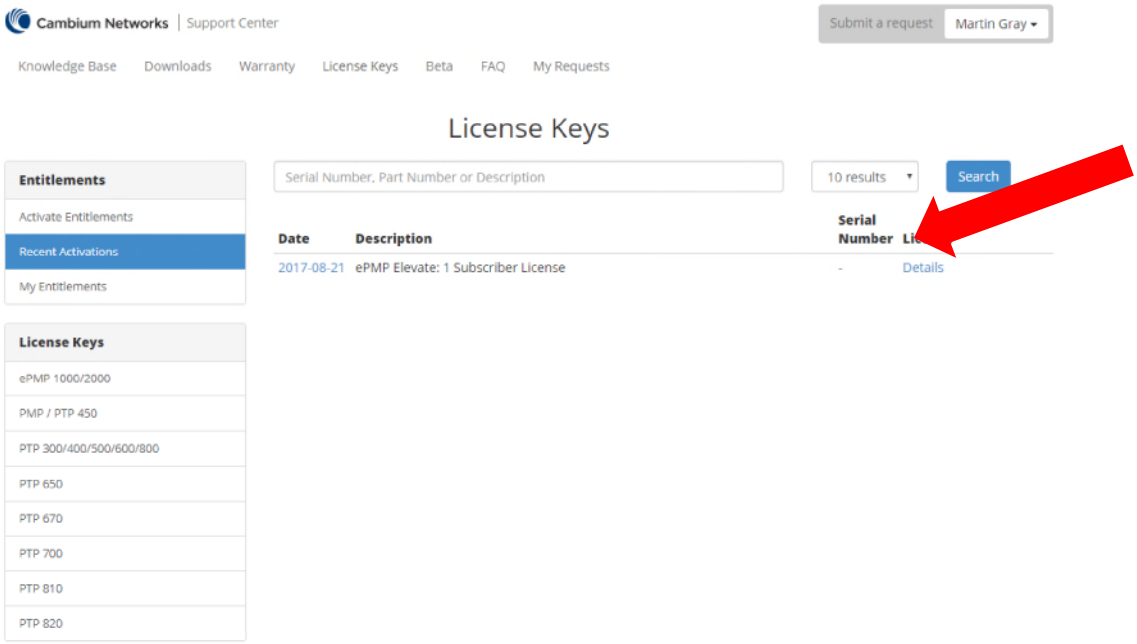
5 Click **Activate** on the resulting page to activate your company account.



6 On the resulting dialogue, enter the number of licenses to activate then click **Activate.**



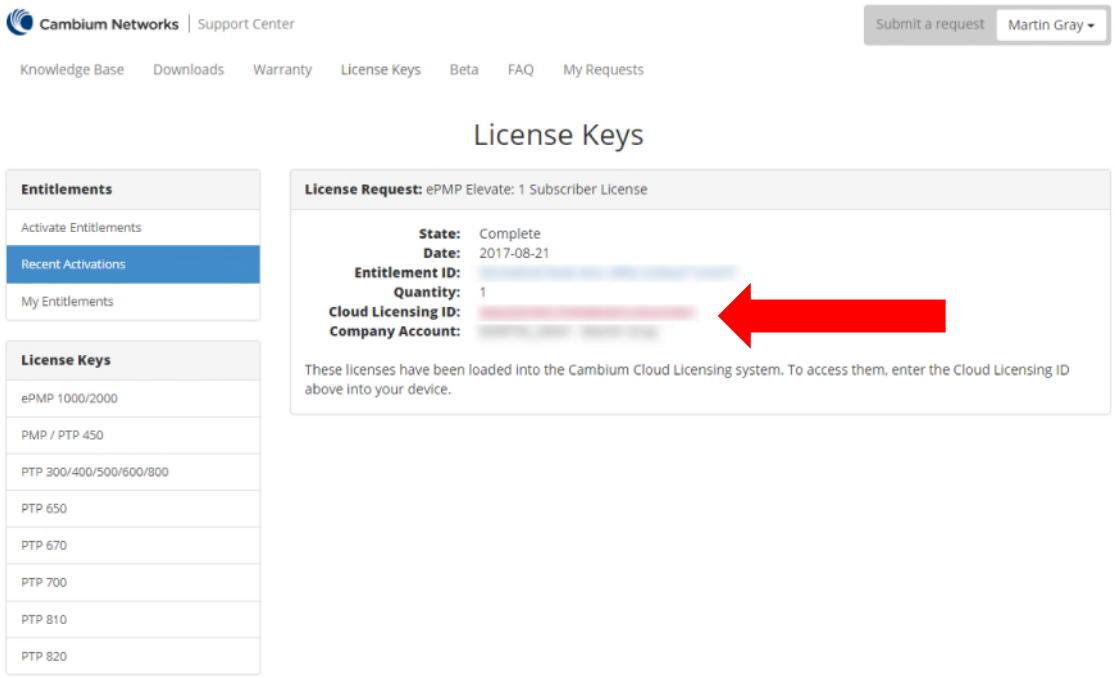
7 The recently-activated license keys are displayed, click **Details** to display the corresponding license key information.



8 To use licenses from the pool, enter the corresponding **Cloud Licensing ID** on the AP's **License Managmenet** page.

Caution

Keep your **Cloud Licensing ID** secret to avoid unintended license pool usage!



ENABLING AP FLEXIBLE LICENSE MANAGEMENT

Procedure:

Follow this procedure to configure the ePMP Access Point to retrieve Elevate licensing information from the Flexible license server.

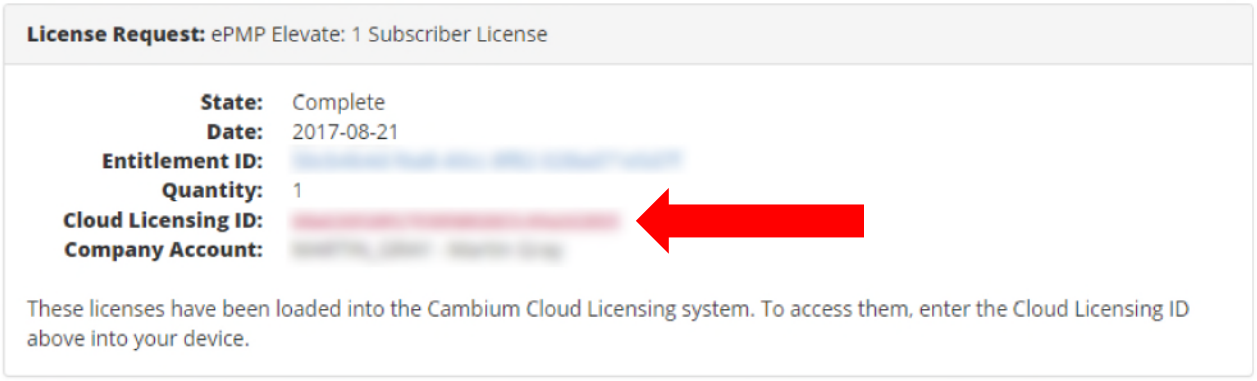
Note

To use flexible licensing, the AP must:

1. be able to make HTTPS requests out to the Internet
2. be running firmware version 3.5.1 or greater
3. have an accurate NTP time source

1 Follow the steps in section Flexible License Generation Procedure on page 12 to activate the applicable licenses on the Cambium Networks Support Center

2 Copy the Cloud Licensing ID generated on the Support Center website



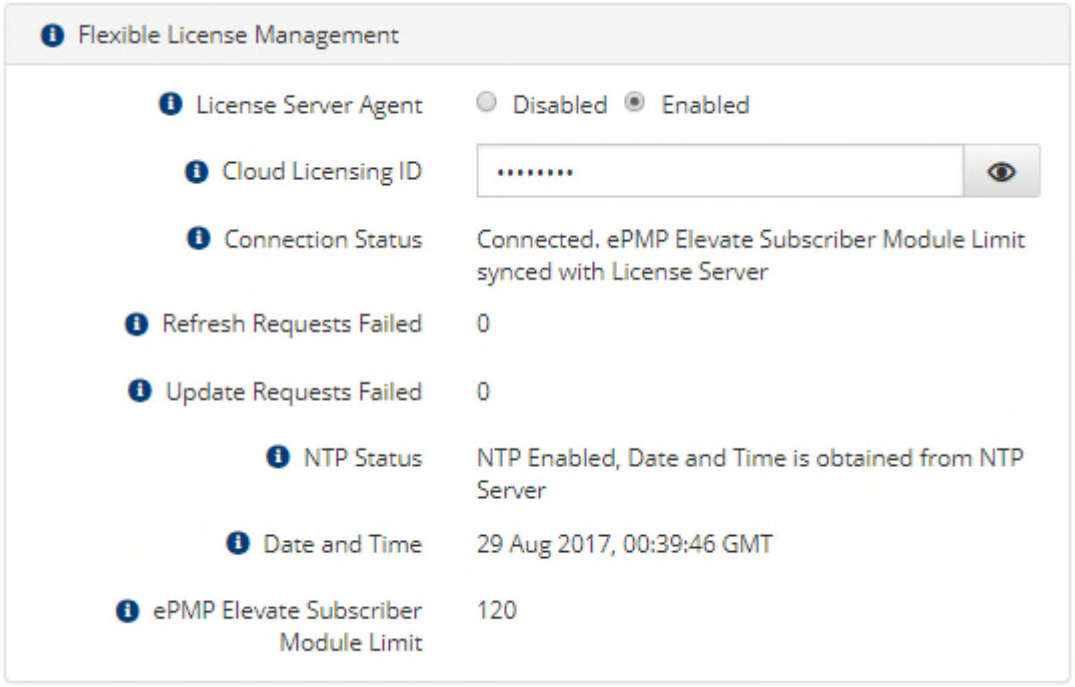
3 Log into the ePMP AP and navigate to **Tools > License Management**

4 Set **License Server Agent** to **Enabled**

5 Paste the **Cloud Licensing ID** from Step 2 into the **Cloud Licensing ID** field

6 Verify the license server connection in with field **Connection Status**

7 Verify the enacted licensing in field **ePMP Elevate Subscriber Module Limit**



Additional Elevate Subscriber Support

For operators of 2.4 GHz networks with ePMP Elevate subscribers, Software Release 3.5.1 introduces support for the following additional hardware types:

- NanoStation Loco M2 (board.sysid = 0xe866)
- NanoStation Loco M2 (board.sysid = 0xe867)

WPA2 Security Vulnerability Fix (KRACK)

Software Release 3.5.1 includes security improvements to prevent Key Reinstallation attacks targeted at ePMP radio networks.

This security improvement includes:

- Prevention of reinstallation of temporal keys (IGTK, GTK) during WPA key handshake

Support for Myanmar Country Code

The Myanmar Country Code is now supported for ePMP with the following operation:

Band	Frequency Range	Valid Center Frequencies 5/10 MHz Channel Size	Valid Center Frequencies 20 MHz Channel Size	Valid Center Frequencies 40 MHz Channel Size	EIRP Limit
2.4 GHz	2400 – 2500 MHz	2407 – 2492 MHz (every 5 MHz)	2412 – 2487 MHz (every 5 MHz)	2422 – 2477 MHz (every 5 MHz)	36 dBm
5.8 GHz	5725 – 5875 MHz	5730 – 5870 MHz (every 5 MHz)	5735 – 5865 MHz (every 5 MHz)	5745 – 5855 MHz (every 5 MHz)	30 dBm

Force 190 ETSI Region DFS Support

Beginning with Software Release 3.5.1, Force 190 devices are supported in ETSI regulatory environments. The Force 190 units use region-specific Dynamic Frequency Selection (DFS) mechanisms based on the device **Country** parameter setting.

 Note

When operating in a region which requires DFS, ensure that the AP (BHM) is configured with alternate frequencies and that the SM (BHS) is configured to scan for these frequencies to avoid long outages.

Defect Fixes (System Release 3.5.1)

Defects in green are resolved
Defects in black are open

Tracking	Description / Workaround
15033	All Elevate SMs except 1 are dropped after upgrade request when Licensed capacity is exceeded
14989 14994	GPS chip information is not displayed with tddstats CLI command
15012	Not possible to upgrade GPS firmware on 2.5 GHz and 6 GHz radios
14970	Unexpected reboot of Force 180 / Force 200 in cold conditions
14928	Spectrum Analyzer terminates after two minutes of operation
14912	[Elevate] NanoStation Loco M2 (board.sysid=0xe867) not supported
14963	[Elevate] NanoStation Loco M2 (board.sysid=0xe866) not supported
14599	IPv6 Gateway not functioning
14921	Latitude and Longitude fields do not accept non-integer values
14558 14935	GUI error when saving RADIUS User Certificate
14894 14770	GUI error when changing device IP Address
14888	[ePMP 2000] LLDP neighbors not detected by ePMP 2000 AP
13790	DHCP Reply from SM may be dropped by AP
12753	DFS Support for Force 190
14945	[Elevate] XM devices in network may have the same Separate Wireless Management Interface MAC address assignments
14910	Radio becomes inaccessible when switching from Bridge to NAT mode with Separate Management IP and Management VLAN enabled
14493	Unable to log into device for 2 minutes after factory default procedure
14922	Myanmar country code support
14839	SNMP MIB parameter sysLocation is not supported
14872	[Elevate] Nanobridge M5 XM always displays Ethernet Port Status as “Down”
14904	IP address of Wireless Gateway obtained from PPPoE server is not displayed on GUI (when Separate Management IP enabled and VLAN retrieved via RADIUS VSA
14918	SNMP sysObjectID does not return Hardware SKU
14887	[Elevate] Software upgrade/downgrade not functional for Elevate XM radios
14968	ePMP key reinstallation attack security improvements

Known Problems or Limitations (System Release 3.5.1)

Tracking	Description / Workaround
15004	[Elevate] AP drops Elevate radio connections when switching from Fixed to Flexible licensing

Tracking	Description / Workaround
14997	Wrong DFS status displayed on ePMP SM Home page when device operates on ETSI non-DFS channel
14962	General error displayed on login page after redirecting to re-configured device IP address Workaround: Reload web page
15016	AP/SM does not obtain IP address via DHCPv6 server
15017	Separate Management IP retrieved from DHCP server after configuring IP Assignment to Static
15007	[Elevate] DNS and Gateway settings may not be carried over when upgrading to ePMP Elevate
15009	SM in NAT mode (Separate Management IP and PPPoE enabled, RADIUS authentication with VLAN VSA retrieval) cannot be upgraded/downgraded, radio connection drops every 10 minutes Workaround: Disable RADIUS authentication
14996	"Applying" is displayed on GUI for an extended period when saving changes on the Security page
15010	[Elevate] Spectrum Analyzer may disconnect after 20 seconds if Static IP Assignment has been modified from original setting Workaround: Click Connect and restart spectrum scan
15006	Satellites table is empty on GPS Gync AP configured in SM mode

Defect Fixes (System Release 3.5)

Tracking	Description / Workaround
14490	[ePMP 2000] Clock calibration between ePMP and ePMP Elevate devices
14455	2nd Management interface obtains Fallback IP with VLAN enabled
14771	Reliable Multicast parameters removed from ePTP mode
14567	[Elevate] Automatic workaround to reset device when Elevate XW Nanostation Loco M5 subscriber Ethernet LAN port goes down
10124	Ethernet watchdog error on SM
14889	"\" symbol for DeviceName crashes web management interface
14721	[Elevate] Unsupported Elevate models removed from MIB file
13308	[Elevate 2.4] RADIUS GUI Authentication not functional
14497	Erroneous validation failure between Lan IP address and Lan Gateway IP addresses
14734	Fixed tcpdump vulnerability to gain root CLI access

Known Problems or Limitations (System Release 3.5)

Tracking	Description / Workaround
14862	Link test error message when run with more than 28 SMs connected to ePMP2000 AP. Workaround: Restart the link test

Tracking	Description / Workaround
14868	Primary Frequency Carrier is not saved to .config file if ACS is started after selecting Country. Workaround: Device reboot or re-run ACS
14866	Save and Undo buttons are highlighted after importing JSON/BINARY configuration with ACS Enabled. Workaround: Web management interface refresh
14872	[Elevate 2.4] ePMP Elevate NanoBridge M2 XM always displays Ethernet Status Down. Display-only issue, Ethernet port is functional. (fixed in 3.5.1)
14846	[Elevate 2.4] Error message 'Please perform device reboot before Upgrading software.' is shown on GUI during SW upgrade. Workaround: Web management interface refresh
14888	LLDP neighbors are not seen by ePMP 2000 AP (fixed in 3.5.1)
14772	"Applying" button is present for a long time in NAT mode if the Community String has changed before. Workaround: Web management interface refresh
14891	"Applying" button is present for a long time if IP address received from DHCP via VLAN interface with enabled LLDP. Workaround: Disable LLDP functionality
14816	Switching IP assignment to Dynamic creates second user GUI session. Workaround: Device reboot
14776	After reset to factory defaults SM in Standard WiFi mode cannot connect to AP configured in Standard WiFi mode on 20 MHz channel bandwidth.
14894	Web management interface shows error message when trying to change IP address. Workaround: Device reboot (fixed in 3.5.1)
14873	Cannot import binary configuration with non-valid License Key.
14904	Wireless Gateway is shown as empty on ePMP SM web management interface if obtained from PPPoE server with Separate Management IP and VSA configured. (fixed in 3.5.1)
14770	New IP Address cannot be assigned if the Community String has been previously changed. Workaround: Device reboot (fixed in 3.5.1)
14906	Unable to force Sector Antenna on ePMP2000 AP via SNMP. Workaround: Use web management interface to force Sector Antenna
14783	Admin password erroneously applied to Full AP radio after exporting configuration from Lite AP radio
14873	Web management interface will not show error after importing binary configuration with non-value license key

Known problems or limitations (System Release 3.4.1)

Tracking	Description / Workaround
14910	Device becomes available after switching from Bridge to NAT mode then enabling Separate Management IP and VLAN. Workaround: Power reset the device (fixed in 3.5.1)
14611	[Elevate 2.4] "SM disassociated from AP. Reason 32/33/48" during Stability test {XW}
14613	Incorrect processing status on GUI when Link Test is failed
14609	Home User erroneously able to configure network configuration (fixed in 3.5)
14614	The Ping utility does not show latency if use less than 8 of 'Buffer Size'

Tracking	Description / Workaround
14612	[Elevate 2.4] Link Test is not completed properly (fixed in 3.5)

Known problems or limitations (System Release 3.4)

Tracking	Description / Workaround
14591	Not able to login to the GUI after changing the IP. Works with Chrome but not with Firefox. However, once you clear the cache and cookies, it works with Firefox. (fixed in 3.4.1) See section **Chrome / Firefox Web Management Interface Access – Special Notice for Software Release 3.4** for additional information.
14589	Upgrade of 2.4 and 5 GHz ePMP Elevate devices to 3.4 will shows as failed when upgraded via cnMaestro. However, the devices do upgrade and a refresh on the cnMaestro screen will show that the devices are running 3.4 after a successful upgrade. (fixed in 3.4.1)
14470	[ePMP Elevate 2.4] Unexpected behaviour of Port Speed Settings
13308	[ePMP Elevate 2.4] RADIUS GUI Authentication: Authentication not functional if used RADIUS authentication method (fixed in 3.5)
14477	DHCP Server on SM sends host name as lease time if only digits are used for DHCP client name
14510	Unable to Export eDetect scan results in Chromium browser with AdBlock extension
14558	GUI shows error message after saving User Certificate for RADIUS Server (fixed in 3.5.1)
14458	[ePMP Elevate 2.4, XM] Cambium Elevate operating Tx Power exceeds original non-Cambium software-configured Tx Power by 1.5 – 3 dBm

Known problems or limitations (System Release 3.3)

Tracking	Description / Workaround
13238	[ePMP Elevate] ePMP Elevate devices are not supported by CNUT
13346	[ePMP Elevate] Device name and network settings are not copied from original device configuration (resolved by ePMP Elevator tool)
13299	[ePMP Elevate] Not possible to configure Uplink Max Rate to any MCS except 7th on single stream devices
14016	After configuring the SM device into NAT mode and reconfiguring the WAN IP address, the Spectrum Analyzer tool is only available via previously-configured Bridge mode IP address
14030	Unable to add new AP to Preferred APs table when in “Show Details” view. As a workaround, add new APs to the table when in “Show List” view. (fixed in 3.4)
14131	[IPv6] AP and SM Separate Management Interface don't display obtained DHCP address on without manual refresh (fixed in 3.4)

Known problems or limitations (System Release 3.2.2)

Tracking	Description / Workaround
13846	It is not possible to change the SM’s Network configuration from Bridge to Router mode via SNMP. (fixed in 3.3)
13825	GUI indicates In-Service-Monitoring DFS status for 5-10 seconds after switching to non-DFS channel.

Known problems or limitations (System Release 3.2.1)

Tracking	Description / Workaround
13783	User cannot login to GUI by DNS address if URL contains dash (-). (fixed in 3.3)
13516	[ePMP Elevate] XM hardware – Spectrum Analyzer not supported (fixed in 3.3)
13343	[ePMP Elevate] XW hardware – If an ePMP Elevate module is interrupted during an ePMP software upgrade, TFTP flash recovery of ePMP Elevate software may fail. As a workaround, load the native device software, then upgrade again to ePMP Elevate
13552	[ePMP Elevate] After changing the device management IP address, the browser may not automatically redirect to the new IP address. Workaround: Enter the new management IP address in the browser address bar. (fixed in 3.3)
13630	[ePMP Elevate] Upon downgrading from Release 3.2.1 to Release 3.2, the Remote Management parameter may be set to Disabled. Workaround: Re-enable the Remote Management parameter after downgrading from Release 3.2.1 to Release 3.2.

Known problems or limitations (System Release 3.2)

Tracking	Description / Workaround
13472	[ePMP Elevate] Updates to XM hardware Ethernet port interface MAC address assignment (fixed in 3.2.1)
13289	Invalid warning appears on web management interface when Subscriber Module Target Receive Level is configured above -60 dBm (fixed in 3.2.1)
13165	SM in NAT mode with Separate Management IP and Management VLAN is not accessible by Separate Management IP address (fixed in 3.2.1)
13228	Web management interface is not accessible after an upgrade attempt with invalid software archive. Workaround: reboot the device to regain management access.
13317	eDetect may not display interfering devices at lower received/detected power levels (fixed in 3.3)
13187	Upon configuration restore, a browser refresh is required to display updated parameter values (fixed in 3.2.1)
13274	[ePMP Elevate] ePMP Elevate subscriber may disconnect under load due to hardware limitations. This disconnect is followed by an immediate re-registration. (fixed in 3.2.2)
12791	[ePMP Elevate] XM devices: When downlink RSSI is stronger than -30 dBm, the web management interface incorrectly reports RSSI of 256 dBm and SNR as 0 dB (fixed in 3.2.1)
12919	[ePMP Elevate] Rocket™ M5 (XM and XW): The web management provides options for configuring the device in AP or ePTP mode. These modes are not supported by ePMP Elevate software and should not be utilized. (fixed in 3.2.1)
13332	On occasion, after upgrading an ePMP SM to Release 3.2, the SM's web management interface may display "Board still in reboot state" or the interface may not be accessible. Workaround: reboot or power cycle the SM. (fixed in 3.3)

Known problems or limitations (System Release 3.1)

Tracking	Description / Workaround
13220	Support for use of shift key to select multiple frequencies in the Scan List (fixed in 3.2.1)
13165	SM does not create static route for separate management interface (fixed in 3.2.1)

Tracking	Description / Workaround
13117	ePMP 2000 device configured in SM mode reports incorrect AP frequency and does not register (fixed in 3.2.1)
12409	With rare occurrence, SM scans without registration
12709	ePMP 2000: Cannot factory default via power cycle sequence (fixed in 3.2.1)
12792	Throughput Chart: Upon changing Throughput Measurement Period, control points (hover targets) not shown (fixed in 3.2.1)
12837	With certain configurations, GPS-synched software can be loaded onto Force 200 module
12878	ePMP device reboots twice after factory default

Known problems or limitations (System Release 3.0.1)

Tracking	Description / Workaround
12385	ePMP web management interface test tool Ping (Tools > Ping) does not execute with maximum buffer size (65507)
12439	ePMP devices with saved cnMaestro credentials which are not on-boarded by cnMaestro for more than 12 hours will stay in state “Device Approval Pending”
12513	Transmitter Output Power reference tables duplicated in web management interface notification

Known problems or limitations (System Release 3.0)

Tracking	Description / Workaround
12794	False radar detection on DFS channel FCC1322 Type1 22 (fixed in 3.2.1)
12793	False radar detection on DFS channel FCC1322 Type1 24 (fixed in 3.2.1)
12125	When in ETSI region and 5.4 GHz band using LBT, if the SM is subjected to very high interference, it may cause a reboot with a crash signature “arqtx_rwb_from_wbuf”.
11973	The “Internet” Globe icon on the top right of the GUI page may take up to 40 seconds to turn green once a DNS server has responded.
11491	When ePMP 2000 is in Standard WiFi, a Ubiquiti Nanobeam may not register. There is currently no workaround.
11406	When using 5 MHz channels on ePMP 2000 in TDD mode, TCP downlink throughput may degrade by up to 20%.

Known problems or limitations (System Release 2.6.2)

Tracking	Description / Workaround
11978	When there are more than 128 entries into the Bridge Table, the table may display as an empty table.

Known problems or limitations (System Release 2.6)

Tracking	Description / Workaround
10907	When in AP WiFi mode and the SM connected is an 802.11a SM, the downlink throughput can be lower by 20%. (fixed in 3.3)
10704	When editing the MAC Addresses entries in the Wireless MAC Filtering table using the configuration file upload, care must be taken to ensure MAC address format integrity. The ePMP device will not validate the format.

Known problems or limitations (System Release 2.4.3)

Tracking	Description / Workaround
9951	On occasion, pings are lost when continuously pinging the SM from the AP. The ping loss can occur for a period of 30-60 seconds before it operates normally. User traffic may also be lost during this time and a reboot of the SM may be required to recover the SM.

Known problems or limitations (System Release 2.4)

Tracking	Description / Workaround
8198	On occasion, stale ARP entries are not cleared from the ARP table (under Monitor>network) on the SM. The entries should be cleared in 5 minutes but it may take up to 10 minutes for them to be cleared.

Technical Support

For technical support, see

http://www.cambiumnetworks.com/support/

Cambium Networks Community Forum

Join the conversation

http://community.cambiumnetworks.com/

Exhibit F

Partial Transcription of November 30, 2016 ePMP Elevate Webinar

**** Webinar may be accessed either at (1) https://www.youtube.com/watch?v=UCxpPmXtp-8 or (2) http://community.cambiumnetworks.com/t5/ePMP-Elevate/ePMP-Elevate-webinar-replay/m-p/62777.***

[Note: Times refer to webinar presentation time]

1:20 – 1:35 – "This is Sakid Ahmed speaking, along with me we have we have Alex Marchum who is the Product Manager of the ePMP program. Dmitry Moiseev, he is a system architecture engineer and a system architect engineer, principal engineer with the ePMP team."

2:26 – Displays slide showing use with Ubiquiti.

3:04 – 3:28 – "Offer a backwards compatibility or interoperability mode for existing subscriber modules that are potentially not Cambium are based on 802.11 n-base subscribers and build a virtual ePMP system where some subscribers are of a different flavor sitting alongside Cambium native ePMP subscribers."

3:35 – Webinar Slide:

- Allows **ePMP Elevate** software to run on **non-Cambium Networks 802.11n-based** subscriber models
- **ePMP Elevate** subscribers function **as ePMP** subscribers – with all the ePMP benefits
- Comparable performance to all-**ePMP** networks, despite different subscriber hardware; industry-first **hardware-agnostic networks**

(Emphasis in original.)

3:39 – 3:52 – "So, with the combination of ePMP and other third party hardware in the same network, this is what we're referring to as the first hardware-agnostic, network solution in the WISP [wireless Internet service provider] industry today."

4:30 – 4:46 – "Many WISPs have existing deployed infrastructure, significant number of subscriber modules from other vendors that are very expensive to replace. So the network, hardware migration still remains very challenging for WISPs today."

4:33 – Webinar Slide (Portion):

- But many WISPs have older deployed gear
  - Network hardware migration remains challenging

4:48 – Webinar Slide:

- Why is network hardware migration **hard?**
  - Cost of **new hardware**
  - **Installation cost** – truck rolls
  - **Customer satisfaction** impact
    - Service credits
    - Arranging installations where indoor access required
    - Downtime and teething troubles

(Emphasis in original.)

8:17 – Webinar Slide (Portion):

- **ePMP Elevate** is the only solution offering a pain-free network migration path to the next level:
  - Frequency re-use enabled by **GPS Synchronization**
  - **Smart Beamforming** and **Intelligent Filtering**
  - All **without** changing subscriber hardware

(Emphasis in original.)

8:58 – 9:11 – "Take your existing hardware that has been stagnant . . . and [have] new life breathed into it with ePMP elevate."

11:35 – Webinar Slide:

- **ePMP Elevate** is first available in **Release 3.2**
- **Release 3.2** consists of:
  - **5 GHz** support only
  - XW-based Ubiquiti hardware (2013 – current)
  - XM-based Ubiquiti hardware (2013 and prior)
  - 17 supported models

11:48 – 12:00 – "We will support XW firmware-based Ubiquiti hardware from 2013-current XM-based Ubiquiti hardware from 2013 and prior, which totals 17 support models today."

12:20 – Webinar Slide:

- **ePMP Elevate** will continue to be developed
- Some future identified items are:
  - **Mikrotik** support
  - Support for more Ubiquiti subscriber modules
  - **2.4 GHz** support

(Emphasis in original.)

12:25 – 12:27 – Goal for future is "support for greater number of Ubiquiti subscriber models."

13:01 – Webinar Slide:

- Lists pricing: ePMP Elevate: 1 Subscriber License $35 (MSRP) (USD)

15:15 – "Live upgrade of a [third party subscriber] unit" (demonstrated by Dmitry Moiseev)

15:53 – 16:14 – "In web browser, you can see the well-known model from Ubiquiti . . . running XW Firmware. What I'm going to do, I'm going just to update it through the regular web update procedure."

18:11– 18:20 – (Video of Ubiquiti Units) "What you see are ePMP 1000 generation subscribers as well as some Ubiquiti subscriber units connected and passing traffic."

21:44 – 21:53 – "Warranty is specific to hardware. ePMP Elevate is a software solution so therefore any hardware specific defects should be reported to the corresponding manufacturer."

25:24 – 25:47 – “Will we be able to use a former Ubiquiti SM and DMS channels? . . . Yes, we will be able to. . . Ubiquiti hardware is DMS approved and it will be available.”

27:07 – 27:15 – “ePMP Elevate solution does not, and I repeat does not replace the plans you have to install new hardware.”

29:42 – 29:54 – “If issue with hardware unit, is it Cambium support issue or Ubiquiti support issue? . . . If it is hardware problem, that is responsibility of hardware manufacturer.”

36:52 – 37:17 – “If you upgrade a subscriber module to ePMP Elevate, you are always able to revert back to the original manufacturer’s software . . . support same hardware reset functionality on all those units and you can always return back to the original manufacture’s software if you so desire. And that answers the question whether the upgrade step is reversible so we won’t go through that again.”

38:25 – 38:30 – “Is there any possibility of Ubiquiti blocking the ability to allow third-party firmware? Absolutely, there is.”

41:29 – Screenshot of Cambium Networks User Interface displaying NanoBeam-M5 with Cambium Networks copyright notice.

47:53 – 47:58 – “Is upgrade reversible and can you move back to Ubiquiti?. . . . Yes, you can.”

48:28 – 48:35 – “Once again warranties are hardware specific so therefore any hardware failures should be referred to the manufacturer.”

49:56 – 50:03 – “Once you’ve uploaded ePMP Elevate . . . old manufacturers’ firmware is not operating in any form.”

Exhibit G

Cambium Networks

ePMP Elevate

Increase performance without replacing installed hardware.

ePMP Elevate is an innovative software solution that empowers 3rd party subscriber hardware with all the performance and scalability benefits of the ePMP platform, when co-installed with an ePMP access point.

Where to Buy

Contact

Get Quote

PMP Distribution

Don't replace your hardware. Elevate it.

Transform your network

ePMP Elevate software solution allows fixed wireless broadband networks to gain the powerful signature capabilities of Cambium Networks' ePMP platform, including frequency reuse enabled by GPS Synchronization and Smart Beamforming, even on non-Cambium 802.11n-based hardware.

The next level of network migration

Saving the cost and time of a total network replacement, an operator simply installs an ePMP Access Point and loads ePMP Elevate software onto their deployed subscriber modules.

Protected investment

With the upgraded features of ePMP Elevate, the life of existing infrastructure is dramatically extended to support revenue-generating applications for years to come.

Contact

Get Quote

Streamlined operations

ePMP Elevate networks can be managed by cnMaestro™, the cloud-based or on-premise platform that provides end-to-end management, device onboarding, and maintenance support for wireless broadband networks from a single, easy-to-use interface.

Managing all your Wireless Devices Effortlessly

See a view from the clouds

With ease of use and vast scalability, cnMaestro has a full set of features targeted to cloud manage Cambium devices in a simple way.

Try cnMaestro Now

Contact

Get Quote

ADDITIONAL RESOURCES

Accessories, including power supplies and antennas

Software downloads and documentation

ePMP Consultants

Community discussion

Technical Training

Recorded Webinars

STAY CONNECTED

Keep up on our always evolving product features and technology.

Enter your email and subscribe to our communications.

Email Address Subscribe

ABOUT US

Mission

Executive Team

Quality

Social Responsibility

CONTACT US

Contact

Get Quote

Careers

Industry Associations

Partners

Office Locations

FOLLOW US

Facebook

YouTube

Twitter

Instagram

Google+

Linkedin

Company Terms and Conditions | Privacy Policy | Cookie Policy | Legal Terms | Email Preferences

Contact

Get Quote

Exhibit H

ROLLING MEADOWS, IL, November 30, 2016 — Cambium Networks, a leading global provider of wireless networking solutions, today announced ePMP™ Elevate, a software solution allowing outdoor wireless broadband networks to gain the powerful signature capabilities of Cambium Networks' ePMP platform, including frequency reuse enabled by GPS Synchronization and Smart Beamforming, even on non-Cambium Networks 802.11n-based hardware. With ePMP Elevate, operators can bring industry-leading performance and scalability to existing infrastructure without the time and cost of replacing network equipment.

As it becomes increasingly important for wireless network operators to keep up with customer demands, the cost and time of traditional network migration methods can be major pain points. The launch of ePMP Elevate takes network migration to the next level, solving the challenges of traditional network migration methods at a fraction of the cost and time. Network operators simply need a single ePMP access point and to load their deployed subscriber modules with ePMP Elevate software. Their hardware investment is protected, and their existing infrastructure is given a new lease on life to support revenue-generating applications for years to come. Additionally, network operators are able to confidently extend high-speed connectivity and increase density to meet customer demand without the time and expense of dispatching technicians to each subscriber location.

“For years we have operated by limiting ourselves to no more than 25 subscribers per AP without seeing a rapid decline in overall AP performance,” said Ian Ellison, CTO, WISPER Internet and Co-Owner of BLIP Networks. “Through prior testing and deployment with ePMP, we knew that GPS synchronization would improve our network stability and spectral efficiency, but we had an equipment and labor investment in the installed base. ePMP Elevate allowed us to achieve synchronization and frequency re-use across our entire network by just replacing the APs. It’s affordable, improves network performance, boosts customer satisfaction, and most importantly allowed us to upgrade our infrastructure without costly truck rolls to replace customer equipment.”

“ePMP Elevate is a software solution that is hardware agnostic,” said Atul Bhatnagar, President and CEO of Cambium Networks. “Network operators with radio hardware from one or multiple vendors can now operate one network with a common management system without replacing installed CPE hardware.”

“Wireless broadband network operators around the world have been asking for this,” said Sakid Ahmed, Vice President, ePMP Business, at Cambium Networks. “Many started out years ago with small networks, but as demand for connectivity has grown, their existing networks cannot effectively scale. ePMP Elevate adds critical features to their 802.11n-based installed equipment and positions them for growth and increased customer satisfaction.”

ePMP Elevate networks can be managed by cnMaestro. This cloud-based or on-premise platform provides end-to-end management, device onboarding, and maintenance support for wireless broadband networks from a single, easy-to-use interface.

Cambium Networks is hosting a free webinar on ePMP Elevate to present the features, benefits, share actual field performance, and discuss deployment strategies. The webinar will be held on Wednesday, November 30, at 9:00 a.m. US CST.

About Cambium Networks:

Cambium Networks is a leading global provider of trusted wireless solutions that connect the unconnected – People, Places and Things. Through its extensive portfolio of reliable, scalable and secure wireless narrowband and broadband platforms, Cambium Networks makes it possible for all service providers and industrial, enterprise and government network operators to build affordable, reliable, high-performance connectivity. The company currently has over six million radios deployed in thousands of demanding networks in more than 150 countries. Headquartered outside Chicago and with R&D centers in the U.S., U.K. and India, Cambium Networks sells through a range of trusted global distributors.

For more information, visit www.cambiumnetworks.com and www.connectingtheunconnected.org.

Share this Post

Email Address Subscribe

ABOUT US

Mission

Executive Team

Quality

Social Responsibility

CONTACT US

Careers

Industry Associations

Partners

Office Locations

FOLLOW US

Facebook

YouTube

Twitter

Instagram

Google+

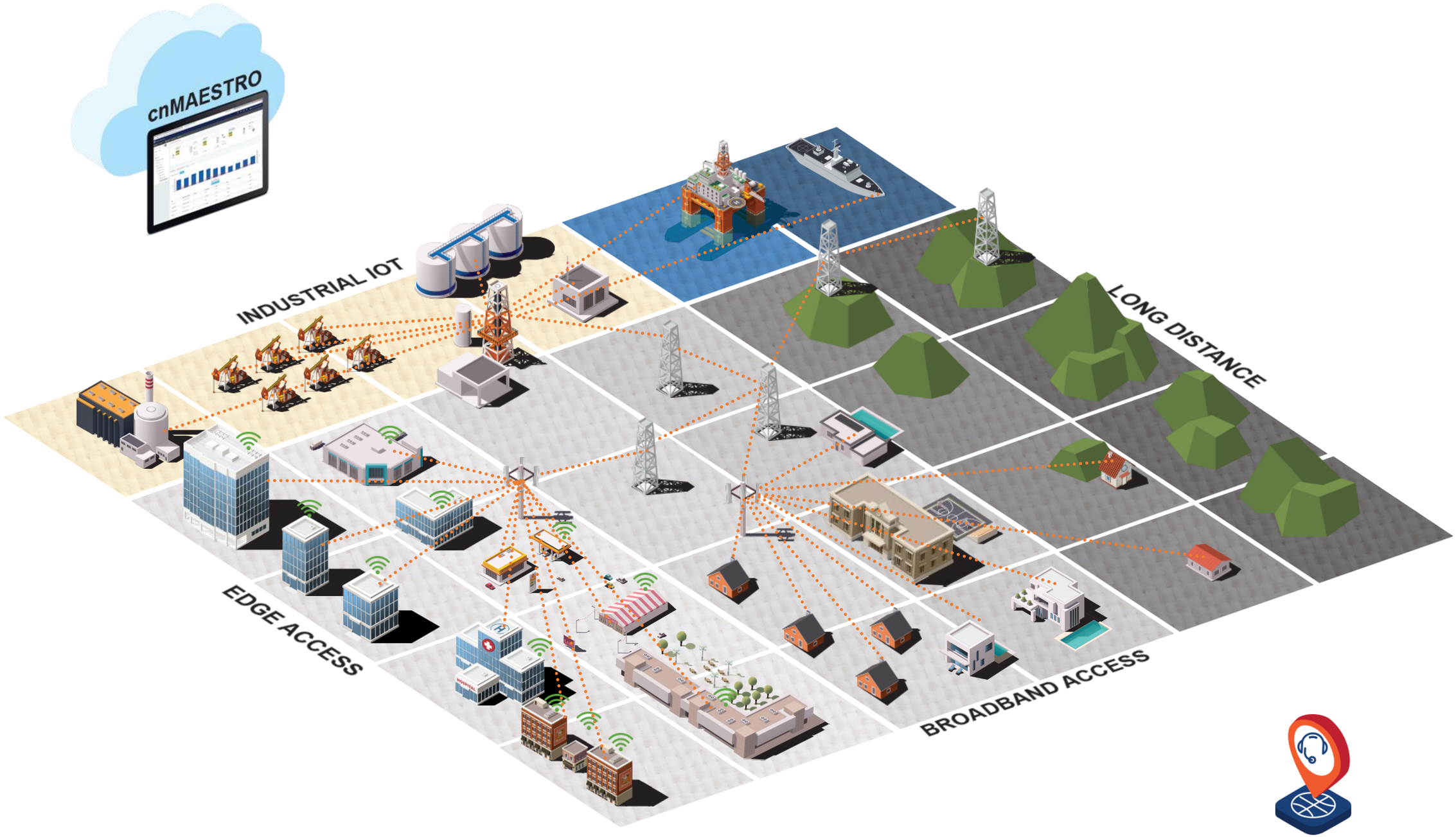
Linkedin

Exhibit I

Cambium Networks™
www.cambiumnetworks.com

Wireless Fabric Connectivity Solutions

Cambium Networks' Wireless Fabric



Breakthrough Technologies

Cambium Networks™
www.cambiumnetworks.com

Cloud and Network Management

LINKPlanner

- Free, network design tool for RF environments
- Tens of thousands of links deployed

cnMaestro

- Cloud management
- Secure, end-to-end network control

cnArcher

- Free android app
- Allows field techs to configure PMP networks

Point-to-Point

PTP 650/670

- Launched in November 2013/2017
- Replacement for legacy PTP 600 which was the “gold standard” for almost a decade

PTP 550

- Launched January 2018
- Exceptional headline data rate (1.4 Gbps)

Point-to-Multipoint

cnMedusa (PMP 450m)

- Launched in September 2016
- Breakthrough 14x14 Massive MU-MIMO
- Will drive continued PMP growth for next several years

PMP 450i

- Launched in September 2012/2016
- Long awaited replacement to flagship PMP product line
- Top performing Cambium product

ePMP

ePMP 1000/2000

- Launched in October 2013
- High quality, affordable platform

ePMP 3000

- Launching December Q2 2018
- 4x4 MU-MIMO & 80 MHz Channel Support
- Higher Capacity and Spectral Efficiency

Wi-Fi

cnPilot e4/5/6xx

- Launched in July 2015, cloud-savvy
- Affordable yet uncompromising quality

cnPilot e430W

- Launching Q1 2018
- Wall Plate AP for Hospitality
- Managed Service Provider enaber

Cambium Networks™
www.cambiumnetworks.com

cnPilot Wi-Fi Portfolio Overview

Provide seamless indoor and outdoor Wi-Fi with field proven solutions that meet capacity needs.




	r190W	r190V	e410	e600	e500	e430W
Key Statement	Indoor residential and small to medium business Wi-Fi access		Enterprise indoor access points		Enterprise outdoor access point with options for antenna coverage: • E500 - omnidirectional • e501S - 90° - 120° • e502S - 30°	Enterprise wall plate
Typical Application	Indoor Wi-Fi coverage • Residential • Small and medium business		Enterprise Wi-Fi coverage for indoor locations: • Enterprise • Hospitality • Industry • Public Wi-Fi • Retail		Wi-Fi coverage for outdoor areas • Enterprise • Hospitality • Industry • Public Wi-Fi	Hospitality
Wi-Fi Standard	802.11n	802.11n	802.11ac Wave 2	802.11ac Wave 2	802.11ac	802.11ac Wave 2
Frequency			2.4 and 5 GHz	2.4 and 5 GHz	2.4 and 5 GHz	2.4 AND 5 GHz
Max Throughput	300 Mbps	300 Mbps	867 Mbps	1.3 Gbps	1.01 Gbps	1.01 Gbps
Tx Power	24 dBm	24 dBm	24 dBm at 2.4 GHz 25 dBm at 5 GHz	24 dBm at 2.4 GHz 28 dBm at 5 GHz	29 dBm at 2.4 GHz 28 dBm at 5 GHz	22 dBm at 2.4 GHz 21 dBm at 5 GHz
Concurrent Users	64	64	256	512	256	256
SSID	4	4	16	16	16	16
Mesh Capability	No	No	Yes	Yes	Yes	Yes
Ethernet ports	4 LAN 1 WAN	4 LAN 1 WAN	1 LAN	2 LAN	2 LAN	3 LAN 1 LAN + PoE
Roaming	No	No	Yes	Yes	Yes	Yes

PMP 450 Platform Overview

Cambium Networks™
www.cambiumnetworks.com

Access Points

450m

5 GHz 450i

3 GHz 450i

450i Connectorized

PMP 450 AP

PMP 450i 900 MHz

900 AP with Sector

900 SM with Yagi

Subscriber Modules

450b Mid-gain

450b High Gain

450i Integrated

450i Connectorized

450 SM Integrated

450 SM with Reflector Dish

Access Points

Subscriber Modules

	450m cnMedusa	450i	450	450b	450i	450
Frequency Bands	3 GHz*, 5 GHz	900 MHz, 3 GHz, 5 GHz	2.4 GHz	3 GHz*, 5 GHz	3 GHz, 5 GHz	900 MHz, 2.4 GHz
Channel Size	5|7|10|15|20|30|40 MHz	5|7|10|15|20|30|40 MHz	5|10|15|20|30|40 MHz	5|7|10|15|20|30|40 MHz	5|7|10|15|20|30|40 MHz	5|7|10|15|20|30|40 MHz
Physical Layer	14 x 14 MU-MIMO / OFDM	2 x 2 MIMO / OFDM	2 x 2 MIMO / OFDM	2 x 2 MIMO / OFDM	2 x 2 MIMO / OFDM	2 x 2 MIMO / OFDM
Interface	Gigabit, SFP 2nd Ethernet port PoE out	Gigabit 2nd Ethernet port PoE out	100 Mbit	Gigabit	Gigabit 2nd Ethernet port PoE out	100 Mbit
Environmental	IP 67, IP 66	IP 67, IP 66	IP 67, IP 66	IP 55 (Mid-gain), IP 67 (High Gain)	IP 67, IP 66	IP 55
Latency	7-10 ms	3-5 ms	3-5 ms	3-5 ms	3-5 ms	3-5 ms
Performance	1.2 Gbps+	300+ Mbps	200+ Mbps	300+ Mbps	300+ Mbps	100+ Mbps
Powering Methods	56V PoE Cambium Proprietary	30V PoE 802.3af	30V PoE Cambium Proprietary Standard PoE Pinouts	30V PoE Cambium Proprietary Standard PoE Pinouts	30V PoE Cambium Proprietary Standard PoE Pinouts	30V PoE Cambium Proprietary Standard PoE Pinouts
Power Consumption	85 W Max, 70 W Typical	19 W Max, 16 W Typical	15 W max, 12 W typical	12 W max, 9 W typical	19 W max, 16 W typical	12 W max, 9 W typical
Max Power	+42 dBm EIRP	+44 dBm EIRP +27 dBm Tx Power	+22 dBm Tx Power	+44 dBm EIRP (mid-gain) +51 dBm EIRP (High gain)	+50 dBm EIRP +27 dBm Tx Power	+22 dBm Tx Power
Antenna	90°/120° Sector	90°/120° Sector: 17 dBi Connectorized or external 60° Sector Antenna (900 MHz)	Connectorized or external 60° Sector Antenna	17 dBi: Mid-Gain 24 dBi: High Gain (5 GHz) 19 dBi: High Gain (3 GHz)*	23 dBi (5 GHz) 19 dBi (3 GHz) Integrated Flat Panel	9 dBi: Integrated (2.4 GHz) Connectorized or external 12 dBi Yagi (900 MHz)
SMs Supported Per Sector	238	238	238			

ePMP™ Portfolio Overview

Cambium Networks™
www.cambiumnetworks.com

ePMP 1000 2.4 GHz

GPS Sync Radio

Connectorized

Integrated

Force 200

ePMP 1000 5 GHz

GPS Sync Radio

Connectorized

Bridge-in-a-Box

Force 180

Force 190

Force 200

ePMP 2000 5 GHz

Access Point with Intelligent Filtering and Sync

ePMP 3000 5 GHz

CSM 300

Q2/18

Force 300-16

Q2/18

Force 300-25

Q4/17

Access Point with MU-MIMO

Q2/18

	Connectorized | Integrated	GPS Sync Radio	Bridge-in-a-Box	Force 180	Force 190	Force 200	Access Point with Intelligent Filtering	Force 300-16 Force 300-25 CSM 300	Access Point with MU-MIMO
Frequency Band(s)	2.4 GHz, 5 GHz 2.4/2.5 GHz (Brazil, NZ) 6.4 GHz (Russia)	2.4 GHz, 5 GHz	5 GHz	5 GHz	5 GHz	2.4 GHz, 5 GHz	*solution with beam steering, intelligent* 5 GHz	5 GHz	5 GHz
Channel Size	5|10|20|40 MHz	5|10|20|40 MHz	5|10|20|40 MHz	5|10|20|40 MHz	5|10|20|40 MHz	5|10|20|40 MHz	5|10|20|40 MHz	20 | 40 | 80 MHz	20 | 40 | 80 MHz
Physical Layer	2 x 2 MIMO / OFDM 802.11n – 64QAM	2 x 2 MIMO / OFDM 802.11n – 64QAM	2 x 2 MIMO / OFDM 802.11n – 64QAM	2 x 2 MIMO / OFDM 802.11n – 64QAM	2 x 2 MIMO / OFDM 802.11n – 64QAM	2 x 2 MIMO / OFDM 802.11n – 64QAM	2 x 2 MIMO / OFDM 802.11n – 64QAM	2 x 2 MIMO / OFDM 802.11ac Wave 2 256QAM	4 x 4 MIMO / OFDM 802.11ac Wave 2 256QAM
Interface	100 Mbit 2nd Ethernet port PoE out	Gigabit	Gigabit	Gigabit	100 Mbit	Gigabit	Gigabit	Gigabit	Gigabit/SFP
Environmental	IP55	IP55	IP55	IP55	IP55	IP55	IP55	IP55	IP55
Latency	15~17ms	5~7ms	15~17ms	5~7ms	2~3ms	2~3ms	5~7ms	5~7ms	5~7ms
Performance	200+ Mbps	200+ Mbps	200+ Mbps	200+ Mbps	200+ Mbps	200+ Mbps	200+ Mbps	600+ Mbps	1+ Gbps
Powering Methods	30V PoE Cambium Proprietary	30V PoE 802.3af	30V PoE Cambium Proprietary Standard PoE Pinouts	30V PoE Cambium Proprietary Standard PoE Pinouts	30V PoE Cambium Proprietary Standard PoE Pinouts	30V PoE Cambium Proprietary Standard PoE Pinouts	56V PoE 802.3at	30V PoE	56V PoE 802.3at
Power Consumption	7 W max, 5 W typical	10 W max, 7.5 W typical	10 W max, 5 W typical	10 W max, 5 W typical	8 W max, 5 W typical	10 W max, 5 W typical	20 W max	12 W	21 W max
Max Tx Power	+30 dBm	+30 dBm	+30 dBm	+30 dBm	+27 dBm	+30 dBm	+30 dBm	+27 dBm	MCS0, VHT80: +25 dBm MCS9, VHT80: +21 dBm
Antenna	Integrated: 2.4 GHz – 11 dBi 5 GHz – 14 dBi Connectorized: 3rd party	90°/120° Sector: 18 dBi or 3rd party antenna	Integrated: 16 dBi	Integrated: 16 dBi	Dish: 22 dBi	Dish: 2.4 GHz - 17 dBi 5 GHz – 25 dBi	90/120° Sector: 17dBi Optional Beamforming	300-16: Integrated 16 dBi 300-25: Dish 25 dBi CSM 300: RP-SMA	90/120° Sector: 17 dBi 4 x 4 MU-MIMO Optional Beamforming
Modes	**AP**: 120 Subscribers **SM** **PTP**	**AP**: 120 Subscribers **PTP**	Bridge-in-a-Box: **PTP**	**SM** **PTP**	**SM** **PTP**	**SM** **PTP**	**AP**: 120 Subscribers **PTP**	**SM** **PTP**	**AP**: 120 Subscribers **PTP**

ePMP elevate

Leverage an existing 802.11-based installed network and add synchronization without the cost of replacing the entire network

Cambium Networks™
www.cambiumnetworks.com

ePMP elevate

Typical Application	Saving the cost and time of a total network replacement, an operator simply installs an ePMP Access Point and loads ePMP Elevate software onto their deployed subscriber modules.
Products Supported	• For Ubiquiti® XW/XM and Mikrotik SXT5-Lite Devices

ePMP 2000
2.4 & 5 GHz

Access Point with Intelligent Filtering and Sync

Industry's most affordable filtering and all the benefits of GPS sync

Access Point with Intelligent Filtering	
Frequency Band(s)	*2.4 &* 5 GHz
Channel Size	5|10|20|40 MHz
Physical Layer	2 x 2 MIMO / OFDM 802.11n – 64QAM
Interface	Gigabit
Performance	200+ Mbps
Powering Methods	56V PoE 802.3at
Power Consumption	20 W max
Max Tx Power	+30 dBm
Antenna	90/120° Sector: 17dBi Optional Beamforming 3rd party horn
Modes	**AP**: 120 Max Subscribers GPS synchronized **PTP** Scheduling: ePTP | TDD | Flexible

Cambium Networks™
www.cambiumnetworks.com

cnReach / IIoT Overview

Simplify the migration to an all-IP network and maximize the use of spectrum while reducing operating costs

N500 900 MHz

N500 700 MHz

N500 450 MHz

N500 220 MHz

N500 I/O Expander

Key Statement	For outdoor critical infrastructure operations, cnReach transports process monitoring and control data from the remote sensor or PLC/RTU back to the operations center supporting real-time automated decision making and on-going analytics. Covering large geographic areas, hard to reach terrain and challenging spectrum environments, cnReach delivers reliable, secure connectivity to the petrochemical, electric utility, water/wastewater/stormwater, rail and transportation industries. cnReach eases the migration to modern networks by combining legacy serial and analog/digital I/O with TCP/IP and Ethernet connectivity.				
Region	NA/CALA/Australia/NZ	US	Global	US	Global
Frequency Bands	ISM mode: 902 - 928 MHz; (915-928 MHz in Australia) MAS mode: 928 - 960 MHz	757-758 MHz and 787-788 MHz	406 – 430 MHz and 450 – 470 MHz	217 – 222 MHz	
Channel Size	ISM: 76 / 154 / 207 / 310 / 600 / 1200 kHz MAS: 12.5 / 25 / 50 kHz	12.5, 25, 50, 100, 200, 250 kHz	12.5 / 25 kHz (50 / 100 kHz available regulations permitting)	12.5 / 15 / 25 / 50 / 100 / 200 kHz	
Modulations	MSK / 2FSK / BPSK / QPSK / 8PSK / 16PSK / 16QAM / 32QAM	MSK / QPSK / 8PSK / 16QAM / 32QAM	MSK / QPSK / 8PSK / 16QAM / 32QAM	MSK / QPSK / 8PSK / 16QAM / 32QAM	
Max Tx Power	Up to 1 W (30 dBm) (ISM) Up to 4 W (36 dBm) (MAS)	Up to 10W (40 dBm)	FCC: 406.1 - 430 MHz (up to 2 W / 33 dBm); 450-470 MHz (up to 8 W / 39 dBm); ETSI: Up to 8W (39 dBm)	217-220: Up to 2W 220-222 Up to 5W	
Adaptive modulation	Yes	Yes	Yes	Yes	
Security	128/256-bit AES encryption and secure management interfaces (HTTPS, SNMPv3)				
Interfaces	Two Ethernet Two Serial (RS-232/422/485) Optional Analog/Digital GPIO	Two Ethernet Two Serial (RS-232/422/485) Optional Analog/Digital GPIO	Two Ethernet Two Serial (RS-232/422/485) Optional Analog/Digital GPIO	Two Ethernet Two Serial (RS-232/422/485) Optional Analog/Digital GPIO	Two Ethernet Two Serial (RS-232/422/485) Analog/Digital GPIO
LINKPlanner	Y	Y	Y	Y	
cnMaestro	Y	Y	Y	Y	

Cambium Networks offers a complete set of accessories for cnReach including power supplies, antennas and adaptors.

Licensed Microwave Overview

Cambium Networks™
www.cambiumnetworks.com

	FULL OUTDOOR		SPLIT MOUNT	
				
	PTP820S	**PTP820C**	**PTP820G + RFU-C**	**PTP820G + RFU-A**
Frequency Band	6 – 38 GHz	6 – 38 GHz	6 – 38 GHz	6, 11 GHz
Channel Size	3.5 - 80 MHz	3.5 - 80 MHz	3.5 - 60 MHz	3.5 - 60 MHz
Number of Carriers	Single	Dual	Single and Dual	Single and Dual
XPIC	Not Supported	Supported	Supported	Supported
MIMO	Not Supported	2x2 / 4x4 MIMO	Not Supported	Not Supported
Traffic Interface	1 x 10/100/1000 Base T (RJ 45)	1 x 10/100/1000 Base T (RJ 45)	4 x 10/100/1000 Base T (RJ 45)	4 x 10/100/1000 Base T (RJ 45)
	2 x 1000 BaseX - SFP	1 x 1000 BaseX - SFP	2 x 1000 BaseX - SFP	2 x 1000 BaseX - SFP
MTU	9600 Bytes	9600 Bytes	9600 Bytes	9600 Bytes
QoS	VLAN ID, p-bits, IPv4, DSCP, IPv6 TC, MPLS EXP	VLAN ID, p-bits, IPv4, DSCP, IPv6 TC, MPLS EXP	VLAN ID, p-bits, IPv4, DSCP, IPv6 TC, MPLS EXP	VLAN ID, p-bits, IPv4, DSCP, IPv6 TC, MPLS EXP
	8 priority queues	8 priority queues	8 priority queues	8 priority queues
	configurable up to 64 Mbit per queue	configurable up to 64 Mbit per queue	configurable up to 64 Mbit per queue	configurable up to 64 Mbit per queue
Configuration	1+0	1+0 to 4+0	1+0 to 2+0	1+0 to 2+0
	1+1 HSB	1+1 / 2+2 HSB	1+1 / 2+2 HSB	1+1 / 2+2 HSB
	2+0, Non-XPIC	2+0 XPIC	2+0 XPIC	2+0 XPIC
		2+2 SD	1+1 HSB with SD	1+1 HSB with SD
Performance (Layer 2)	596 Mbps - No Compression	1.2 Gbps - No Compression	1 Gbps - No Compression	1 Gbps - No Compression
	833 - Multi-Layer Compression	2 Gbps - Multi-Layer Compression	2 Gbps - Multi-Layer Compression	2 Gbps - Multi-Layer Compression
Modulation	QPSK to 2048 QAM w/ACM	QPSK to 2048 QAM w/ACM	QPSK to 2048 QAM w/ACM	QPSK to 2048 QAM w/ACM
Multi Carrier Link Aggregation	N/A	MC-ABC	MC-ABC	MC-ABC
Power Consumption	6-11 GHz: 40W	6 & 11 GHz: 65W	IDU: 23.5W(single modem)	IDU: 23.5W(single modem)
		7 GHz: 75W	IDU: 26.4W(Dual modem)	IDU: 26.4W(Dual modem)
	13-38 GHz: 35W	13-15 GHz & 26-38 GHz: 55W	RFU-C 6-26 GHz: 22W (1+0), 39W (1+1)	RFU-Ae: 77W (1+0), 101W(1+1)
		18-24 GHz: 48W	RFU-C 28-38 GHz: 26W (1+0), 43W (1+1)	RFU-Aep: 90W (1+0), 114W(1+1)
Maximum Tx Power	29 dBm	28 dBm	26 dBm	35 dBm

Cambium Networks™
www.cambiumnetworks.com

Point to Point Sub 6 GHz: Product at a Glance






	Bridge-in-a-Box	F300-25	PTP 450	PTP 450i	PTP 550 (Dual Carrier)	PTP 670
Frequency Range (GHz)	4.9 to 5.97	5.15 to 5.97	3.5 /3.65/ 5.4 to 5.8 GHz	4.90 to 5.925	5.15 – 5.97	4.9 to 6.05
Channel BW (MHz)	5/10/20/40	20/40/80	5/10/20/30	5/10/15/20/30/40	2x 20/40/80	5/10/15/20/30/40/45
Technology	802.11n	802.11ac Wave 2	Proprietary	Proprietary	802.11ac Wave 2	Proprietary
Line of Sight	LoS	LoS	LoS	LoS	LoS	LoS, nLoS, NLoS
Environmental	IP55	IP55	IP55	IP66/67	IP66/67	IP66/67
Latency	3-6 ms	3-6 ms	3-5 ms	3-5 ms	3-5 ms	1-3 ms
Performance	200 Mbps	600 Mbps	300 Mbps	300 Mbps	1.4 Gbps	450 Mbps
Top Modulation	64 QAM	256 QAM	256 QAM	256 QAM	256 QAM	256 QAM
Max Frame Size	1700 Bytes	1700 Bytes	1700 Bytes	1700 Bytes	1700 Bytes	9600 Bytes
Spectrum Management	Standby Spectrum Analyzer	Live Spectrum Analyzer	Standby Spectrum Analyzer	Standby Spectrum Analyzer	Dynamic Channel Selection	Dynamic Spectrum Optimization (DSO)
Dynamic Filter	No	No	No	Yes	No	No
IEEE 1588v2 & SyncE	No	No	No	No	No	Yes
TDD Sync	No	No	Yes	Yes	Yes	Yes
Encryption	AES 128	AES 128	AES 128	AES 128	AES 128	AES 128/AES 256
QOS	3 Level	3 Level	2 Level	4 Level	3 Level	8 Levels
Power Consumption	7W	12 W	12 W	< 25 W	< 25 W	<30 W
Max Tx Power	30 dBm	27 dBm	22 dBm	27 dBm	27 dBm	27 dBm
Integrated Antenna	16 dBi	25 dBi or 16 dBi	14 dBi	23 dBi	23 dBi	23 dBi

Planning and Management Overview

Cambium Networks™
www.cambiumnetworks.com

LINKPlanner

Quickly design networks for optimal deployment and cost effectiveness with ease.

cnArcher

Raise the bar on installation accuracy with cnArcher™, the free Android app that gives field techs the information they need to configure and properly align Cambium Networks PMP wireless broadband subscriber modules.

cnMaestro

cnMaestro™ is a cloud-based or on-premises software platform for secure, end-to-end network control.

Typical Application	LINKPlanner allows you to model scenarios – based on geography, distance, antenna height, transmit power, and other factors – to optimize system performance before purchase. Quickly design networks for optimal deployment and cost effectiveness with ease. Available for Microsoft® Windows® and Mac® systems, LINKPlanner is a free, user-friendly link-design tool.	Designed with input from field technicians and years of experience on our millions of wireless broadband modules deployed, cnArcher validates configuration and alignment in seconds. Increase the number of installs done right the first time, and increase customer satisfaction. Eliminate problems, and focus your manpower on connecting new subscribers as your network grows.	cnMaestro wireless network manager simplifies device management by offering full network visibility. View and perform a full suite of wireless network management functions in real time. Optimize system availability, maximize throughput, and meet emerging needs of business and residential customers.
Products Supported	• cnPilot • ePMP • PMP • PTP • cnReach	• PMP	• cnPilot • ePMP • cnReach

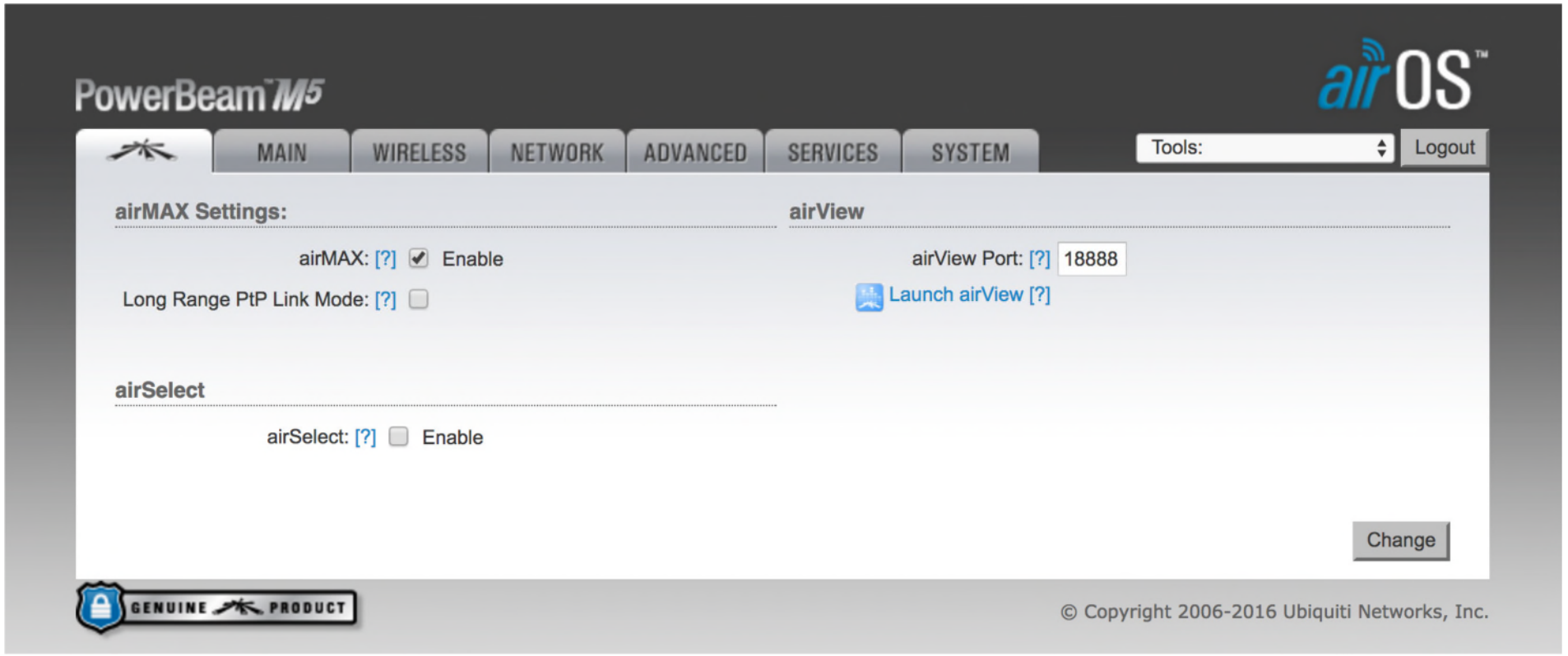
Cambium Networks Wireless Network Fabric

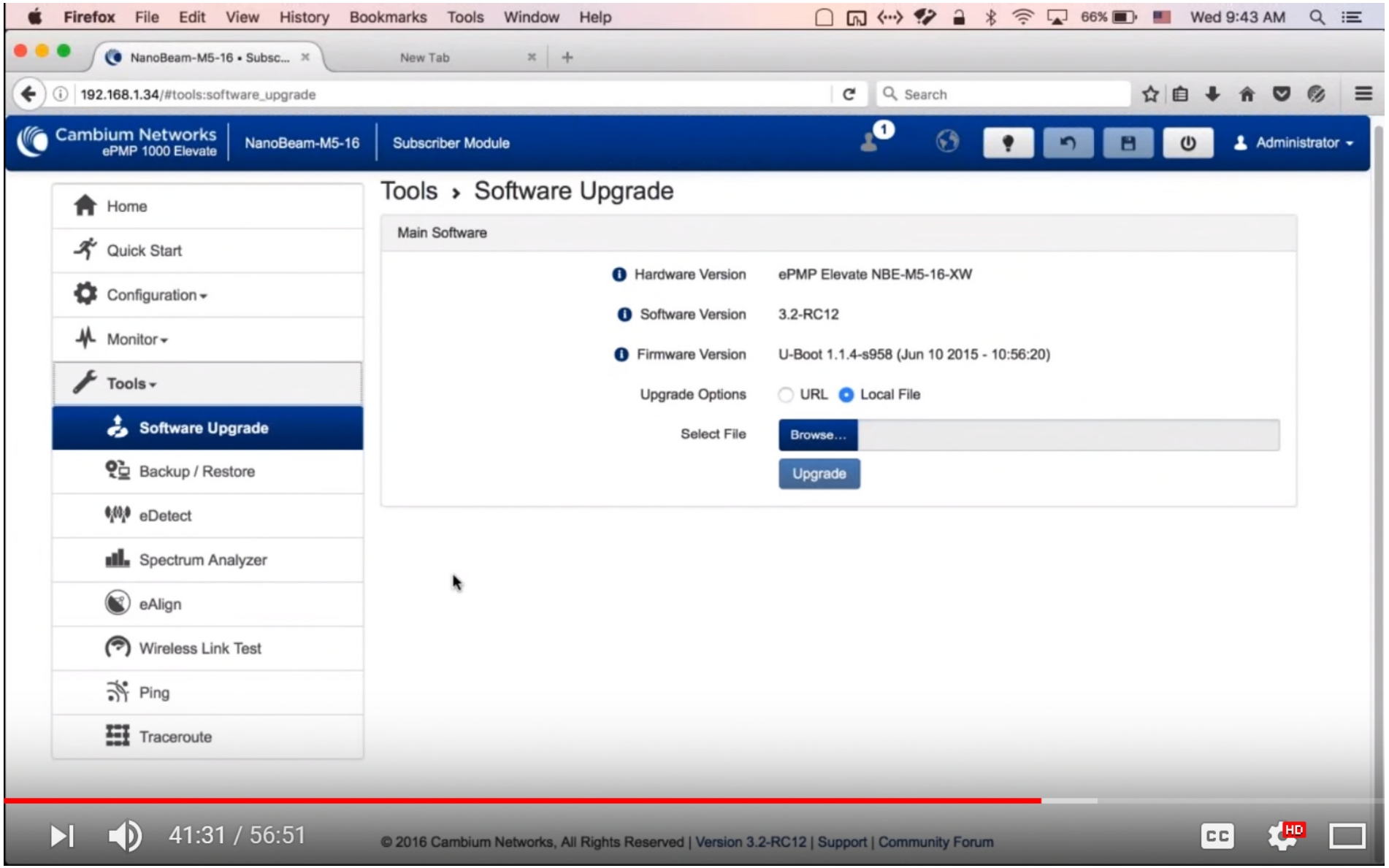
Cambium Networks™
www.cambiumnetworks.com

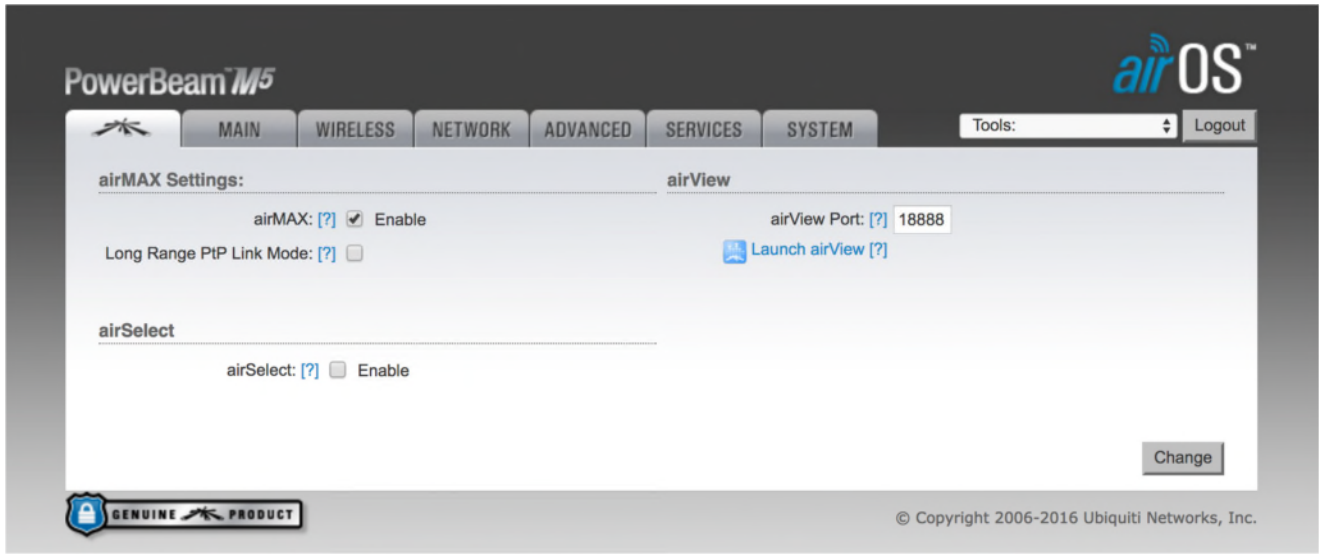
- People Places Things
- Purpose Built
- 2m to 246km
- Kb to Mb to Gb
- Indoor and Outdoor
- PTP PMP Wi-Fi LTE
- Licensed and Unlicensed
- Scalable
- Concept to Commissioning
- Single Pane of Glass

Resilient, Efficient, Affordable Wireless Connectivity Solutions

Exhibit J


PowerBeam M5
airOS
MAIN
WIRELESS
NETWORK
ADVANCED
SERVICES
SYSTEM
Tools:
Logout
airMAX Settings:
airMAX: [?] Enable
Long Range PtP Link Mode: [?]
airView
airView Port: [?] 18888
Launch airView [?]
airSelect
airSelect: [?] Enable
Change
GENUINE PRODUCT
© Copyright 2006-2016 Ubiquiti Networks, Inc.


Firefox File Edit View History Bookmarks Tools Window Help
Wed 9:43 AM
NanoBeam-M5-16 • Subsc...
New Tab
192.168.1.34/#tools:software_upgrade
Search
Cambium Networks
ePMP 1000 Elevate
NanoBeam-M5-16
Subscriber Module
Administrator
Home
Quick Start
Configuration
Monitor
Tools
Software Upgrade
Backup / Restore
eDetect
Spectrum Analyzer
eAlign
Wireless Link Test
Ping
Traceroute
Tools › Software Upgrade
Main Software
Hardware Version
ePMP Elevate NBE-M5-16-XW
Software Version
3.2-RC12
Firmware Version
U-Boot 1.1.4-s958 (Jun 10 2015 - 10:56:20)
Upgrade Options
URL
Local File
Select File
Browse...
Upgrade
41:31 / 56:51
© 2016 Cambium Networks, All Rights Reserved | Version 3.2-RC12 | Support | Community Forum
CC
HD


PowerBeam M5
airOS
MAIN
WIRELESS
NETWORK
ADVANCED
SERVICES
SYSTEM
Tools:
Logout
airMAX Settings:
airMAX: [?] Enable
Long Range PtP Link Mode: [?]
airView
airView Port: [?] 18888
Launch airView [?]
airSelect
airSelect: [?] Enable
Change
GENUINE PRODUCT
© Copyright 2006-2016 Ubiquiti Networks, Inc.

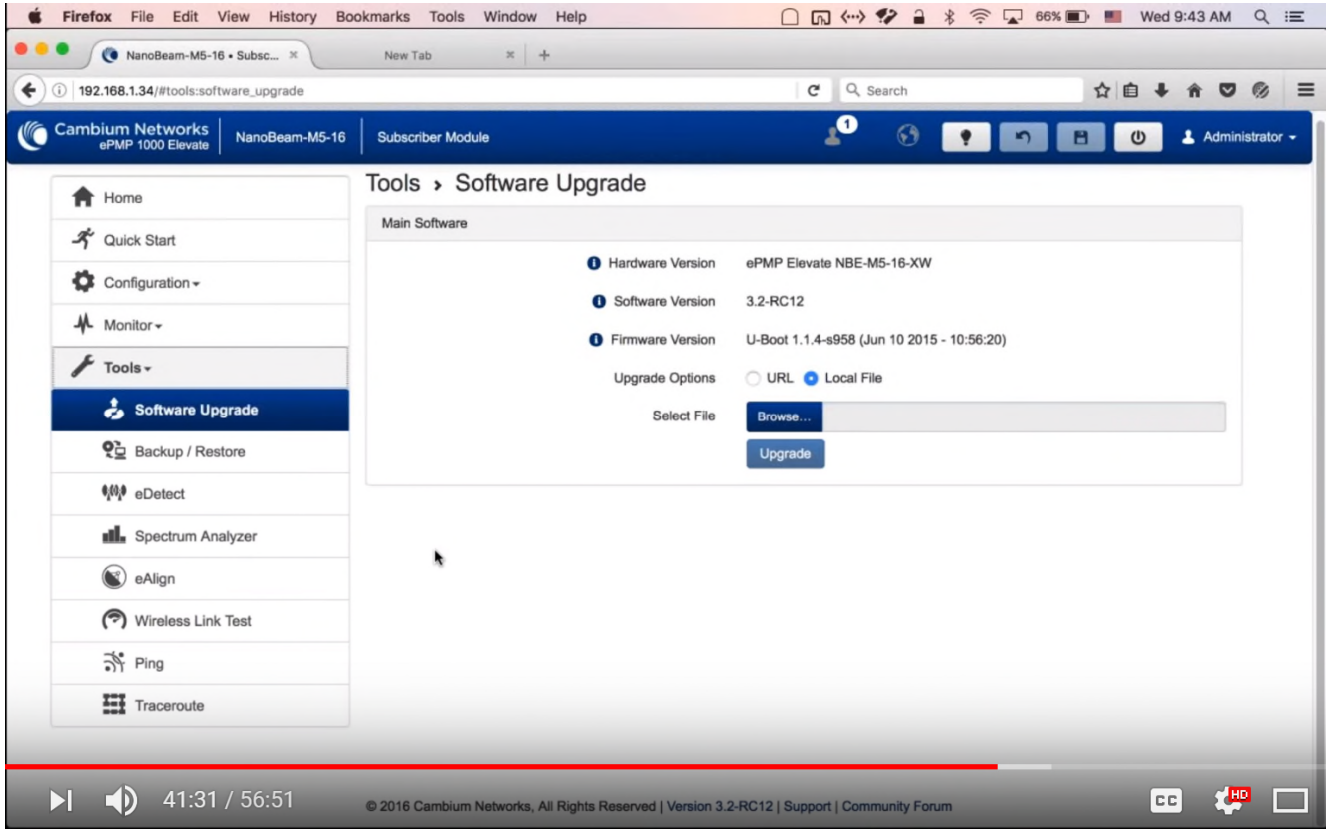

Firefox File Edit View History Bookmarks Tools Window Help
Wed 9:43 AM
NanoBeam-M5-16 • Subsc...
New Tab
192.168.1.34/#tools:software_upgrade
Search
Cambium Networks
ePMP 1000 Elevate
NanoBeam-M5-16
Subscriber Module
Administrator
Home
Quick Start
Configuration
Monitor
Tools
Software Upgrade
Backup / Restore
eDetect
Spectrum Analyzer
eAlign
Wireless Link Test
Ping
Traceroute
Tools › Software Upgrade
Main Software
Hardware Version
ePMP Elevate NBE-M5-16-XW
Software Version
3.2-RC12
Firmware Version
U-Boot 1.1.4-s958 (Jun 10 2015 - 10:56:20)
Upgrade Options
URL
Local File
Select File
Browse...
Upgrade
41:31 / 56:51
© 2016 Cambium Networks, All Rights Reserved | Version 3.2-RC12 | Support | Community Forum
CC
HD

Exhibit K

Issues elevating Ubiquiti devices with firmware higher than 5.6.15

SOLVED

Go to solution

georgehbb Occasional Contributor 10-06-2017 09

Issues elevating Ubiquiti devices with firmware higher than 5.6.15

Hi Everyone,

We are trying to elevate some devices here in the office before we test them in the field.
We could easily elevate Nanostations 2.4, but we are having issues with the PowerBeams.
I made sure we were using the XW firmware, I did read a bunch of forum discussions about it. I also tried to use the **elevator tool** available at this link:
https://www.dropbox.com/sh/2ja5jwsids1p9k8/AAAFMn_Us8qlnMBaMbM5FFW

La?dl=0

Tried with different Elevate firmwares:
From XW 3.5 to XW 3.2

Unfortunately the Ubiquiti interface says:

> This firmware is not trusted by airOS. To maintain security, it will not be loaded. Please load trusted firmware.

I tried to upgrade the Powerbeam to 6.1.0 and downgrade it to 5.6.15 (the lowest firmware Ubiquiti would allow you to use) to no success.

Any suggestion? Thank you.

Solved! Go to Solution.

0 Kudos Reply

2 REPLIES

All forum topics ‹ Previous Topic Next Topic ›

CAMBIUM Luis Cambium Employee 10-06-2017 02

Re: Issues elevating PowerBeam 2.4 with firmware 5.6.15

Hello,

Please check this thread to see if it helps your situation.

Regards

2 Kudos Reply

georgehbb Occasional Contributor 10-10-2017 09

Re: Issues elevating PowerBeam 2.4 with firmware 5.6.15

I found the solution myself. I hope this will help others in my same situation.

The bottom line here is that AS OF NOW (please check the date of this post) you CANNOT downgrade a ubiquiti device to a firmware lower than 5.6.15.

In order to elevate a Ubiquiti device you need to have it (ideally) on 5.6.6

Some guy from Nepal shared some BETA firmware that allowes you to downgrade any device to 5.6.6
I put the file on this link https://www.justbeamit.com/mz6rr

Procedure: (works on both XM and XW)

1) Downgrade device to 6.0.6 beta

2) Downgrade to 6.0.4 (beta)

3) Downgrade to regular 5.6.6

4) Install elevate firmware (3.5 it's the most updated as of now)

Works like charm

You will be able to elevate any Nanostation or PowerBeam by following this procedure.

2 Kudos

Reply

Top

Ubiquiti new firmware 6.0.6 is trying to put stop on Elevate plans?

jperez Occasional Contributor 07-10-2017 07

Ubiquiti new firmware 6.0.6 is trying to put stop on Elevate plans?

the release notes of the new firmware looks like Ubiquiti trying to stop Elevate plans.

```
6.0.6 (XM/XW/TI) Changelog / July 5, 2017
====

New:
- Signed firmware support (Users are not able to downgrade below v6.0.6 unless
using TFTP)
- Upgrade libpcap to 1.8.1
- Additional statistics for AC2 agent
```

0 Kudos Reply

5 REPLIES

All forum topics ‹ Previous Topic Next Topic ›

Chris_Bay Valued Contributor 07-10-2017 08

Re: Ubiquiti new firmware 6.0.6 is trying to put stop on Elevate plans?

Figured they would at soms point.... im sure elivate took a lot of business from them.

0 Kudos Reply

Eric Ozrelic Trusted Contributor 07-10-2017 11

Re: Ubiquiti new firmware 6.0.6 is trying to put stop on Elevate plans?

There is a work-around at the moment... if you've already loaded 6.0.6 final onto a radio, you can load 6.0.6 beta, and then you can load 6.0.4 which will allow you to upload Elevate. You can find the beta HERE. You can find 6.0.4 HERE.

Please note that with 6.0.6 beta, UI firmware downgrades are restricted to 5.6.15, 6.0.3 and 6.0.4

1 Kudo Reply

mohannadda1996 New Member 07-21-2017 12

Re: Ubiquiti new firmware 6.0.6 is trying to put stop on Elevate plans?

I cant download beta version.....

22312.jpg 161 KB

0 Kudos Reply

Mike99 Contributor

07-25-2017 10

Re: Ubiquiti new firmware 6.0.6 is trying to put stop on Elevate plans?

> Chris_Bay wrote:
> im sure elivate took a lot of business from them.

The radio is already sold so it's hard to took buisness in this case but it could slow the old technology replacement. Anyway, N vs AC difference is not enough to worth changing gears but MU-MIMO could worth it.

0 Kudos

Reply

fgoldstein Contributor

07-25-2017 10

Re: Ubiquiti new firmware 6.0.6 is trying to put stop on Elevate plans?

To download the 6.0.6-beta, you first have to sign up for the beta program. Instructions on on UBNT's forums. They're giving that out as general advice, not just ot people who normally woudl try a beta.

0 Kudos

Reply

Top

Exhibit L

December 4, 2017

Promotion - ePMP Elevate licenses for free !!!

References

Home page
About company
Contacts

news
Equipment
Solutions
Resources

Cambium Networks is launching a campaign to help owners of wireless networks built on Ubiquiti equipment to upgrade their network by replacing old equipment with the base station of the ePMP1000 or ePMP 2000 series. When purchasing new ePMP equipment, you get Elevate licenses as a gift !!!

EPMP Elevate is an inexpensive, easy and fast way to significantly increase the performance of an existing wireless broadband access network deployed on 802.11n equipment.

There is no need to replace the subscriber devices! You change only your old access point to the high-performance Cambium base station series ePMP1000 or ePMP2000!

When buying a base of 2.4 GHz or 5 GHz ePMP 1000 - 10 free licenses Elevate!
When buying a base 5 GHz ePMP 2000 Access Point (AP) - 20 free licenses Elevate!
When buying a base 5 GHz ePMP 2000 Access Point + sector antenna + bimforming antenna - 30 free Elevate licenses!

The promotion is valid until December 31, 2017!

More detailed information about the action is available on request, which can be sent by mail to sales@winncom.ru , or by leaving a message in the form of a feedback below:

Your name*

Your surname *

Company*

Your email *

Phone*

Question*

4 Декабря 2017

Акция – лицензии ePMP Elevate бесплатно!!!

Ссылки

- Главная страница
- О компании
- Контакты
- Новости
- Оборудование
- Решения
- Ресурсы

Компания Cambium Networks проводит акцию, призванную помочь владельцам беспроводных сетей, построенных на оборудовании Ubiquiti, модернизировать свою сеть, заменив старое оборудование на базовую станцию серий ePMP1000 или ePMP 2000. При покупке нового оборудования ePMP вы получаете лицензии Elevate в подарок!!!

Программа ePMP Elevate – недорогой, простой и быстрый способ значительного увеличения производительности существующей сети беспроводного широкополосного доступа, развернутой на оборудовании стандарта 802.11n.

При этом нет необходимости в замене абонентских устройств! Вы меняете только вашу старую точку доступа на высокопроизводительную базовую станцию Cambium серии ePMP1000 или ePMP2000!

- **При покупке базы 2.4 GHz or 5 GHz ePMP 1000 – 10 бесплатных лицензий Elevate!**
- **При покупке базы 5 GHz ePMP 2000 Access Point (AP) – 20 бесплатных лицензий Elevate!**
- **При покупке базы 5 GHz ePMP 2000 Access Point + секторная антенна + бимформинг антенна – 30 бесплатных лицензий Elevate!**

Акция действует до 31 декабря 2017 года!

Более подробная информация об акции предоставляется по запросу, который можно направить по почте на адрес sales@winncom.ru, или оставив сообщение в форме обратной связи ниже:

Ваше имя*

Ваша фамилия*

Компания*

Ваш email*

Телефон*

Вопрос*

Я прочитал(а) и согласен(а) с Политикой конфиденциальности

Отправить